Get started

NetApp Ransomware Resilience

NetApp
December 03, 2025

Table of Contents

Get started

Learn about NetApp Ransomware Resilience

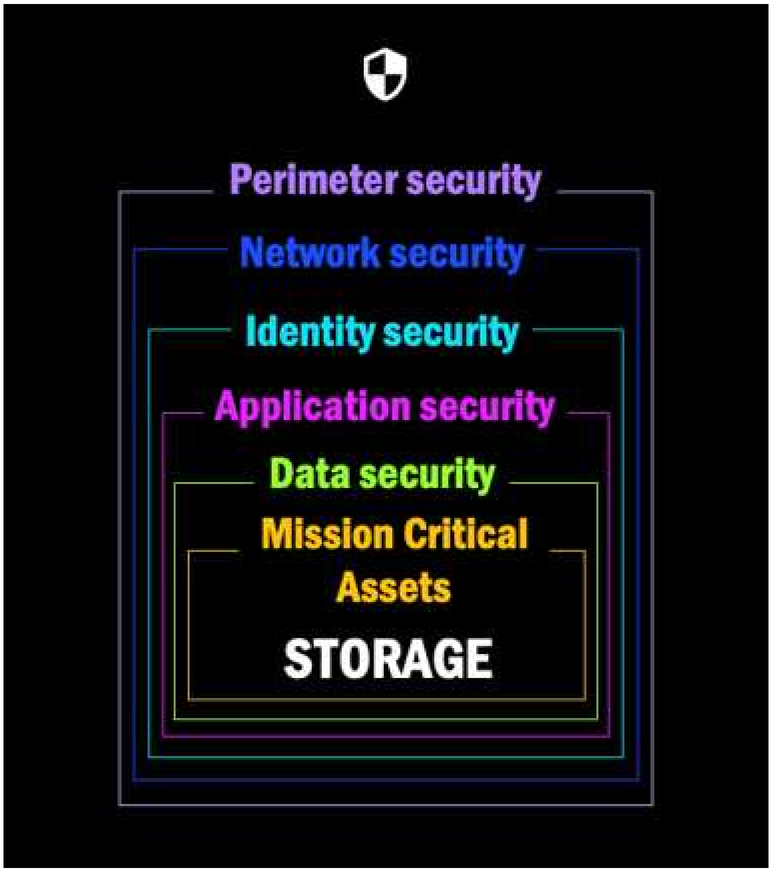
Ransomware attacks can block access to your data and attackers can ask for ransom in exchange for the release of data or decryption. According to the IDC, it is not uncommon for victims of ransomware to experience multiple ransomware attacks. The attack can disrupt access to your data for anywhere from one day to several weeks.

NetApp Ransomware Resilience protects your data from ransomware attacks. In Ransomware Resilience, protection is available for application-based workloads of Oracle, MySQL, VM datastores, and file shares on on-premises NAS storage (using the NFS and CIFS protocols) and SAN storage (FC, iSCSI, and NVMe) as well as Cloud Volumes ONTAP for Amazon Web Services, Cloud Volumes ONTAP for Google Cloud, Cloud Volumes ONTAP for Microsoft Azure, and Amazon FSx for NetApp ONTAP across the NetApp Console. You can back up data to Amazon Web Services, Google Cloud, Microsoft Azure cloud storage, and NetApp StorageGRID.

Ransomware Resilience at the data layer

Your security posture typically encompasses multiple layers of defense to protect against a range of cyber threats.

- **Outermost layer**: This is your first line of defense using firewalls, intrusion detection systems, and virtual private networks to safeguard network boundaries.
- **Network security**: This layer builds upon the foundation with network segmentation, traffic monitoring, and encryption.
- **Identity security**: Uses authentication methods, access controls, and identity management to ensure only authorized users can access sensitive resources.
- **Application security**: Protects software applications using secure coding practices, security testing, and runtime application self-protection.
- **Data security**: Safeguards your data with data protection, backups, and recovery strategies. Ransomware Resilience operates on this layer.



What you can do with Ransomware Resilience

Ransomware Resilience provides full use of several NetApp technologies so that your storage administrator, data security administrator, or security operations engineer can accomplish the following goals:

- **Identify** all application-based, file-share, or VMware-managed workloads in NetApp on-premises NAS (NFS or CIFS) and SAN (FC, iSCSI, and NVMe) systems across the NetApp Console, projects, and Console agents. Ransomwware Resilience categorizes the data priority and provides recommendations to you for ransomware resilience improvements.
- **Protect** your workloads by enabling backups, snapshot copies, and ransomware protection strategies on your data.
- **Detect** anomalies that might be ransomware attacks. [1]
- **Respond** to potential ransomware attacks by automatically initiating a tamper-proof NetApp ONTAP snapshot that is locked so that the copy cannot be deleted accidentally or maliciously. Your backup data will stay immutable and protected end to end from ransomware attacks at the source and in the destination.
- **Recover** your workloads that help accelerate workload uptime by orchestrating several NetApp technologies. You can choose to recover specific volumes. Ransomware Resilience provides recommendations on the best options.
- **Govern**: Implement your ransomware protection strategy and monitor the outcomes.

Benefits of using Ransomware Resilience

Ransomware Resilience offers the following benefits:

- Discovers workloads and their existing snapshot and backup schedules, and ranks their relative importance.
- Evaluates your ransomware protection posture and displays it in an easy-to-understand dashboard.
- Provides recommendations on next steps based on discovery and protection posture analysis.
- Applies AI/ML-driven data protection recommendations with one-click access.
- Protects data in top application-based workloads, such as MySQL, Oracle, VMware datastores and file-shares.
- Detects ransomware attacks on data in real time on primary storage using AI technology.
- Initiates automated actions in response to detected potential attacks by creating snapshot copies and initiating alerts about abnormal activity.
- Applies curated recovery to meet RPO policies. Ransomware Resilience orchestrates recovery from ransomware incidents by using several NetApp recovery services, including NetApp Backup and Recovery (formerly Cloud Backup) and SnapCenter.
- Uses role-based access control (RBAC) to govern access to features and operations.

Cost

NetApp doesn’t charge you for using the trial version of Ransomware Resilience.

> ⓘ With the October 2024 release, new deployments of Ransomware Resilience offer a 30-day free trial. Previously, Ransomware Resilience provided a 90-day free trial. If you’ve enrolled already in the 90-day free trial, that trial is valid for the 90 days.

If you have both Backup and Recovery and Ransomware Resilience, any common data protected by both products is billed by Ransomware Resilience only.

After you purchase a license or PayGo subscription, any workload that has a ransomware detection policy (Autonomous Ransomware Protection) enabled (discovered or set by Ransomware Resilience), and at least one snapshot or backup policy, Ransomware Resilience classifies it "Protected" and it counts against purchased capacity or the PayGo subscription. If a workload is discovered without a detection policy even if it has backup or snapshot policies, it is classified “At risk” and it does *not* count against purchased capacity.

Protected workloads count against purchased capacity or the subscription after the 90-day trial period ends. Ransomware Resilience is charged on a per GB basis for the data associated with protected workloads before efficiencies.

Licensing

With Ransomware Resilience, you can use different licensing plans including a free trial, a pay-as-you-go subscription, or bring your own license.

Ransomware Resilience requires a NetApp ONTAP One license.

The Ransomware Resilience license does not include additional NetApp products. Ransomware Resilience can use Backup and Recovery even if you don’t have a license for it.

To detect anomalous user behavior, Ransomware Resilience uses NetApp Autonomous Ransomware Protection, a machine learning (ML) model within ONTAP that detects malicious file activity. This model is included in the Ransomware Resilience license.

For details, see Set up licensing.

NetApp Console

Ransomware Resilience is accessible through the NetApp Console.

The NetApp Console provides centralized management of NetApp storage and data services across on-premises and cloud environments at enterprise grade. The Console is required to access and use NetApp data services. As a management interface, it enables you to manage many storage resources from one interface. Console administrators can control access to storage and services for all systems within the enterprise.

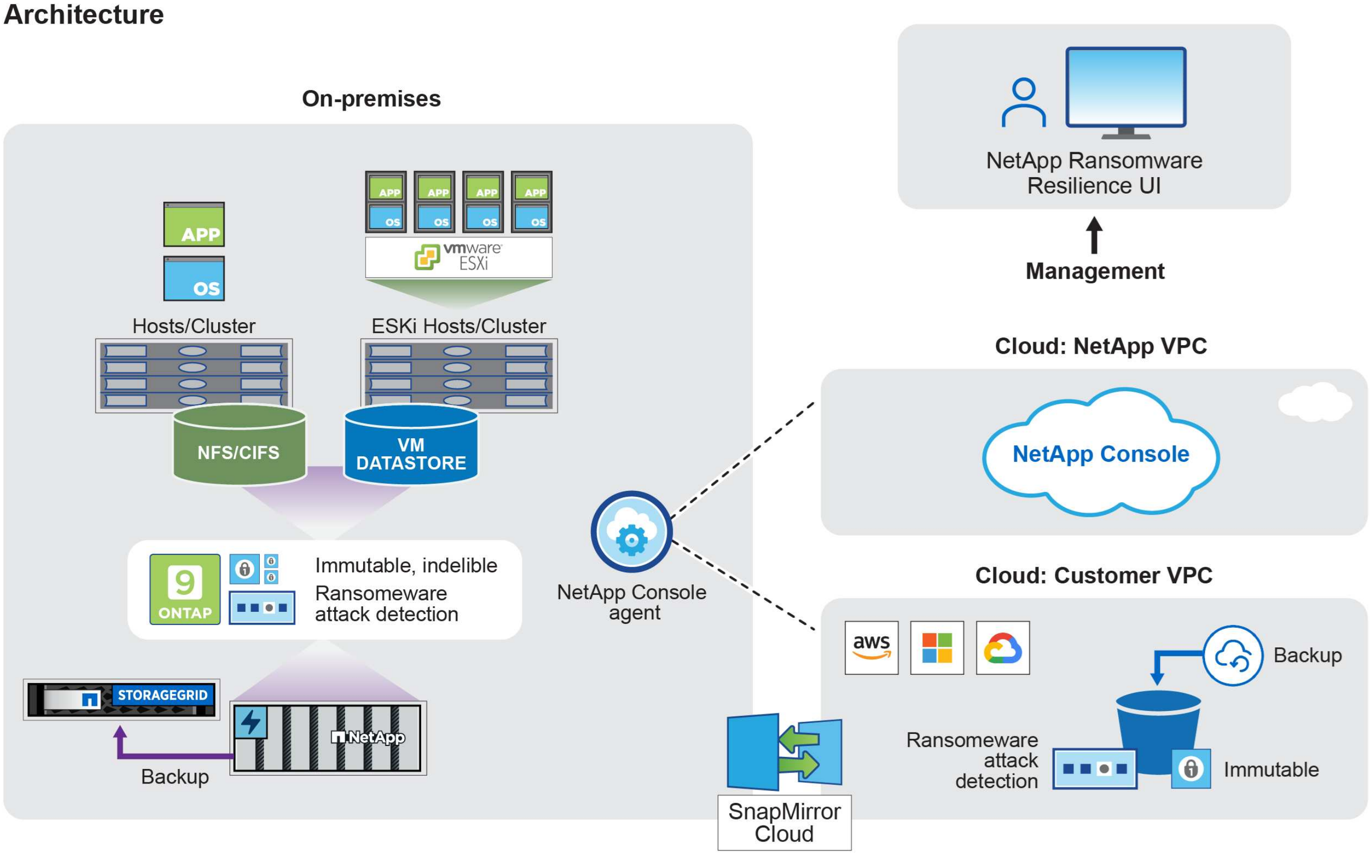
You don’t need a license or subscription to start using NetApp Console and you only incur charges when you need to deploy Console agents in your cloud to ensure connectivity to your storage systems or NetApp data services. However, some NetApp data services accessible from the Console are licensed or subscription-based.

Learn more about the NetApp Console.

How Ransomware Resilience works

Ransomware Resilience uses NetApp Backup and Recovery to discover and set snapshot and backup policies for file share workloads, and SnapCenter or SnapCenter for VMware to discover and set snapshot and backup policies for application and VM workloads. In addition, Ransomware Resilience uses Backup and Recovery and SnapCenter / SnapCenter for VMware to perform file- and workload-consistent recovery.

Architecture



Feature	Description
IDENTIFY	• Finds all customer on-premises NAS (NFS and CIFS protocols), SAN (FC, iSCSI, and NVMe), and Cloud Volumes ONTAP data connected to the Console. • Identifies customer data from ONTAP and SnapCenter service APIs and associates it with workloads. Learn more about ONTAP and SnapCenter Software. • Discovers each volume’s current protection level of NetApp snapshot copies and backup policies as well as any on-box detection capabilities. Ransomware Resilience then associates this protection posture with the workloads by using Backup andRrecovery, ONTAP services, and NetApp technologies such as Autonomous Ransomware Protection (ARP or ARP/AI depending on your ONTAP version), FPolicy, Backup policies, and snapshot policies. Learn more about Autonomous Ransomware Protection, NetApp Backup and Recovery, and ONTAP FPolicy. • Assigns a business priority to each workload based on automatically discovered protection levels and recommends protection policies for workloads based on their business priority. Workload priority is based on snapshot frequencies already applied to each volume associated with the workload.
PROTECT	• Actively monitors workloads and orchestrates the use of Backup and Recovery, SnapCenter, and ONTAP APIs by applying policies to each of the identified workloads.
DETECT	• Detects potential attacks with an integrated machine learning (ML) model that detects potentially anomalous encryption and activity. • Provides dual-layer detection that starts with detecting potential ransomware attacks in the primary storage and responding to abnormal activities by taking additional automated snapshot copies to create the nearest data restore points. Ransomware Resilience provides the ability to dig deeper to identify potential attacks with greater precision without impacting the performance of the primary workloads. • Determines the specific suspect files and maps that attack to the associated workloads, using ONTAP, Autonomous Ransomware Protection (ARP or ARP/AI depending on your ONTAP version) and FPolicy technologies.
RESPOND	• Shows relevant data, such as file activity, user activity, and entropy, to help you complete forensic reviews about the attack. • Initiates quick snapshot copies by using NetApp technologies and products such as ONTAP, Autonomous Ransomware Protection (ARP or ARP/AI depending on your ONTAP version), and FPolicy.
RECOVER	• Determines the best snapshot or backup and recommends the best recovery point actual (RPA) by using Backup and Recovery, ONTAP, Autonomous Ransomware Protection (ARP or ARP/AI depending on your ONTAP version), and FPolicy technologies and services. • Orchestrates the recovery of workloads including VMs, file shares, block storage, and databases with application consistency.

Feature	Description
GOVERN	• Assigns the ransomware protection strategies • Helps you monitor the outcomes.

Supported backup targets, systems, and workload data sources

Ransomware Resilience supports the following backup targets, systems, and data sources:

Supported backup targets

- Amazon Web Services (AWS) S3
- Google Cloud Platform
- Microsoft Azure Blob
- NetApp StorageGRID

Supported systems

Environment	Protocol	Supported versions
Amazon FSx for NetApp ONTAP*	NFS, CIFS, and SAN	N/A
Cloud Volumes ONTAP for AWS	CIFS & NFS	9.11.1 and later
	SAN (FC, iSCSI, & NVMe)	9.17.1 and later
Cloud Volumes ONTAP for Google Cloud Platform	CIFS & NFS	9.11.1 and later
	SAN (FC, iSCSI, & NVMe)	9.17.1 and later
Cloud Volumes ONTAP for Microsoft Azure	CIFS & NFS	9.12.1 and later
	SAN (FC, iSCSI, & NVMe)	9.17.1 and later
ONTAP (on-premises)	CIFS & NFS	9.11.1 and later
	SAN (FC, iSCSI, & NVMe)	9.17.1 and later

* Amazon FSx for NetApp ONTAP uses Autonomous Ransomware Protection (ARP) and not ARP/AI. For more information about the difference, see ARP/AI.

> ⓘ Using ARP/AI in ONTAP requires ONTAP 9.16 or greater.
> ONTAP doesn’t provide ransomware protection support for FabricPool FlexCache, FlexGroup volumes, consistency groups mount point volumes, mount path volumes, offline volumes, and Data protection (DP) volumes. Ensure you review supported and unsupported configurations in ONTAP.

Supported workload data sources

Ransomware Resilience protects the following application-based workloads on primary data volumes:

- Block storage
- Databases:

  - Microsoft SQL Server
  - MySQL
  - Oracle
  - PostgreSQL
- NetApp file shares
- VMware datastores

If you’re using SnapCenter or SnapCenter for VMware, all workloads supported by those products are also identified in Ransomware Resilience. Ransomware Resilience can protect and recover these in a workload-consistent manner.

Terms that might help you with ransomware protection

You might benefit by understanding some terminology related to ransomware protection.

- **Protection**: Protection in Ransomware Resilience means ensuring that snapshots and immutable backups occur on a regular basis to a different security domain using protection policies.
- **Workload**: A workload in Ransomware Resilience can include MySQL or Oracle databases, VMware datastores, or file shares.

NetApp Ransomware Resilience prerequisites

Get started with NetApp Ransomware Resilience by verifying the readiness of your operational environment, network access, and web browser.

To use Ransomware Resilience, ensure you meet the prerequisites.

Supported systems

Ensure you’re using a supported system:

Environment	Protocol	Supported versions
Amazon FSx for NetApp ONTAP*	NFS, CIFS, and SAN	N/A
Cloud Volumes ONTAP for AWS	CIFS & NFS	9.11.1 and later
	SAN (FC, iSCSI, & NVMe)	9.17.1 and later
Cloud Volumes ONTAP for Google Cloud Platform	CIFS & NFS	9.11.1 and later
	SAN (FC, iSCSI, & NVMe)	9.17.1 and later
Cloud Volumes ONTAP for Microsoft Azure	CIFS & NFS	9.12.1 and later
	SAN (FC, iSCSI, & NVMe)	9.17.1 and later
ONTAP (on-premises)	CIFS & NFS	9.11.1 and later
	SAN (FC, iSCSI, & NVMe)	9.17.1 and later

* Amazon FSx for NetApp ONTAP uses Autonomous Ransomware Protection (ARP) and not ARP/AI. For more information about the difference, see ARP/AI.

NetApp Console requirements

Your NetApp Console configuration requires:

- A NetApp Console user account with Organization Admin privileges for discovering resources.
- A Console organization and system with at least one active Console agent connecting to a supported system.
  - If your on-premises ONTAP clusters or Cloud Volumes ONTAP in AWS or in Azure cloud are not set up in the Console, see Learn how to configure a Console agent and standard Console requirements.

    ⓘ If you have multiple Console agents in a single Console organization, the Ransomware Resilience will scan ONTAP resources across all Console agents beyond the one that is currently selected in the Console UI.

- The Console agent must have the `cloudmanager-ransomware-protection` container in an active state.
- At least one Console system with a NetApp on-premises ONTAP cluster or Cloud Volumes ONTAP in AWS or Azure. Ransomware Resilience supports both NAS (NFS and SMB) and SAN (iSCSI, FC, and NVMe) protocols.
  - Ransomware Resilience is supported with ONTAP or Cloud Volumes ONTAP clusters with ONTAP version 9.11.1 or greater.

    ⓘ To use Ransomware Resilience on SAN workloads, you must be running ONTAP 9.17.1 or later.

ONTAP requirements

- You must be running ONTAP 9.11.1 or later with an ONTAP One license enabled on the on-premises ONTAP instance. For more information about ONTAP support, see Autonomous Ransomware Protection overview.
- To apply protection configurations (such as enabling Autonomous Ransomware Protection), Ransomware Resilience needs admin permissions on the ONTAP cluster. The ONTAP cluster should have been onboarded using ONTAP cluster admin user credentials only.

ⓘ If you've connected an ONTAP cluster to the Console with non-admin credentials, [you must update the credentials in the ONTAP cluster](#update-non-admin-user-permissions-in-an-ontap-system).

Data backups

- An account in NetApp StorageGRID, AWS S3, Azure Blob, or Google Cloud Platform for backup targets with appropriate access permissions configured.

  Refer to the AWS, Azure, or S3 permissions list for details.

- NetApp Backup and Recovery does not need to be enabled on the system.

  Ransomware Resilience helps configure a backup destination through the Settings option. See Configure settings.

Suspicious user behavior

For Ransomware Resilience to provide alerts about suspicious user behavior, you must configure a user activity agent. For more information, see Configure suspicious user activity detection in NetApp Ransomware Resilience.

Update non-admin user permissions in an ONTAP system

If you need to update non-admin user permissions for a particular system, complete these steps.

1. Log in to the Console and look for the system that needs its ONTAP user permissions updated.
2. Select the system to see details.
3. Select **View additional information** to display the username.
4. Log in to the ONTAP cluster CLI as an admin user.
5. Display the existing roles for that user. Enter:

   ```
   security login show -user-or-group-name <username>
   ```

6. Change the role for the user. Enter:

   ```
   security login modify -user-or-group-name <username> -application
   console|http|ontapi|ssh|telnet -authentication-method password -role
   admin
   ```

7. Return to the NetApp Console to use Ransomware Resilience.

Quick start for NetApp Ransomware Resilience

Understand the high-level steps you need to follow to set up Ransomware Resilience and protect your workloads.

Follow the links in each step for detailed information.

1

Review prerequisites

These tasks require the *Console admin* role.

- Ensure you've installed a Console agent
- Ensure your system meets the requirements
- Review Ransomware Resilience user roles and assign permissions to users accessing Ransomware Resilience
- Set up licensing

2

Get started with Ransomware Resilience

These tasks require the *Ransomware Resilience admin* role.

- Discover workloads in the Console
- View workload protection health on the Dashboard
- Optionally, conduct a ransomware attack readiness drill

❸ Configure protection and detection in Ransomware Resilience

These tasks require the *Ransomware Resilience admin* role. Configuring suspicious user behavior activity requires the additional *Ransomware Resilience user behavior admin* role.

- Protect workloads
  - Optionally, enhance protection by configuring suspicious user activity detection
- Optionally, configure backup destinations:
  - Prepare NetApp StorageGRID, Amazon Web Services, Google Cloud Platform, or Microsoft Azure as a backup destination.
  - Configure backup destinations
- Respond to detection of potential ransomware attacks
- Recover from an attack (after incidents are neutralized)

❹ What’s next?

After you configure protection in Ransomware Resilience, here’s what you might do next.

- Enable Data Classification to identify governance and security risks
- Send alerts to SIEM
- Download alert, protection, readiness drill, recovery, or summary reports

Set up NetApp Ransomware Resilience

You can easily deploy NetApp Ransomware Resilience. Before you begin, review prerequisites to ensure that your environment is ready.

Prepare the backup destination

Prepare one of the following backup destinations:

- NetApp StorageGRID
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

After you configure options in the backup destination itself, you will later configure it as a backup destination in Ransomware Resilience. For details about how to configure the backup destination in Ransomware Resilience, refer to Configure backup destinations.

Prepare StorageGRID to become a backup destination

If you want to use StorageGRID as your backup destination, refer to StorageGRID documentation for details about StorageGRID.

Prepare AWS to become a backup destination

- Set up an account in AWS.
- Configure AWS permissions in AWS.

For details about managing your AWS storage in the Console, refer to Manage your Amazon S3 buckets.

Prepare Azure to become a backup destination

- Set up an account in Azure.
- Configure Azure permissions in Azure.

For details about managing your Azure storage in the Console, refer to Manage your Azure storage accounts.

Set up the NetApp Console

The next step is to set up the Console and Ransomware Resilience.

Review Console requirements for standard mode.

Create a Console agent

Contact your NetApp Sales Rep to try out or use this service. Then, when you use the Console agent, it will include the appropriate capabilities for Ransomware Resilience.

To create a Console agent using Ransomware Resilience, contact your Console organization admin who has permissions to create Console agents, and refer to the documentation that describes how to create a Console agent.

> ⓘ If you have multiple Console agents, the Ransomware Resilience scan datas across all Console agents beyond the one that currently shows in the Console. This service discovers all projects and all Console agents associated with this organization.

Access NetApp Ransomware Resilience

Log in to NetApp Ransomware Resilience through the NetApp Console.

To log in to the Console, you can use your NetApp Support Site credentials or you can sign up for a NetApp cloud login using your email and a password. Learn more about logging in.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, Ransomware Resilience admin, or Ransomware Resilience viewer role. Learn about Ransomware Resilience roles for NetApp Console.

Steps

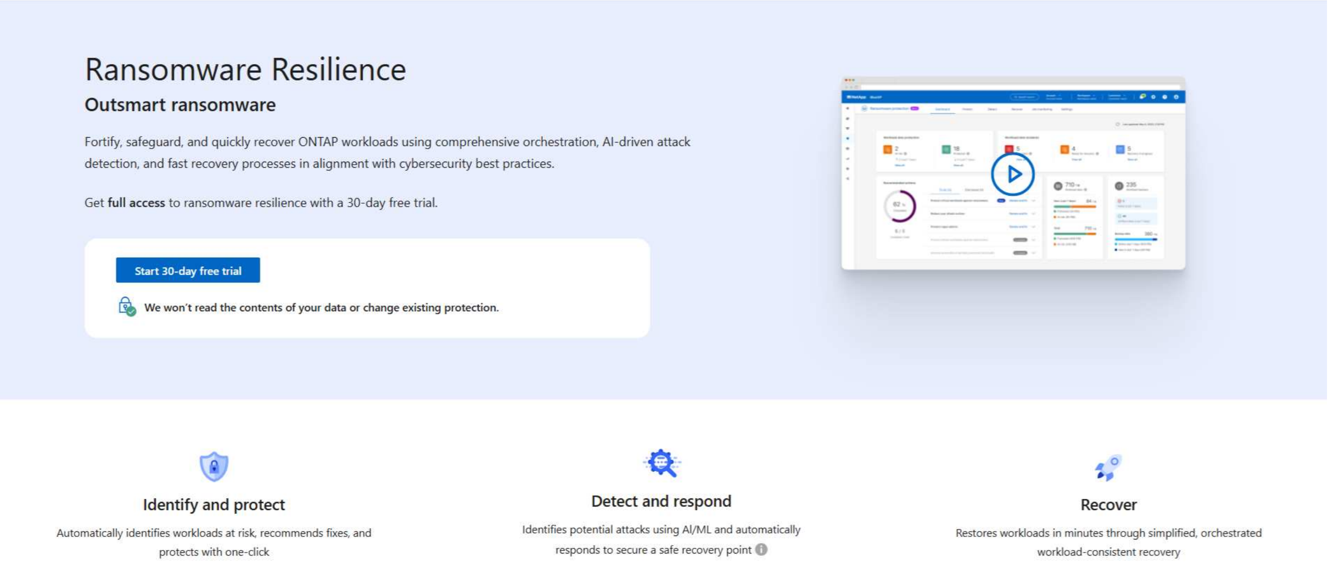
1. Open a web browser and go to the Console.

The Console login page appears.

2. Log in to the Console.
3. From the Console left navigation, select **Protection** > **Ransomware Resilience**.

   If this is your first time logging in to this service, the landing page appears.

   > ⓘ If you don’t have a Console agent or it’s not the one for this service, you need to deploy one. Learn how to set up a Console agent.



Ransomware Resilience

Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get **full access** to ransomware resilience with a 30-day free trial.

Start 30-day free trial

We won’t read the contents of your data or change existing protection.

Identify and protect

Automatically identifies workloads at risk, recommends fixes, and protects with one-click

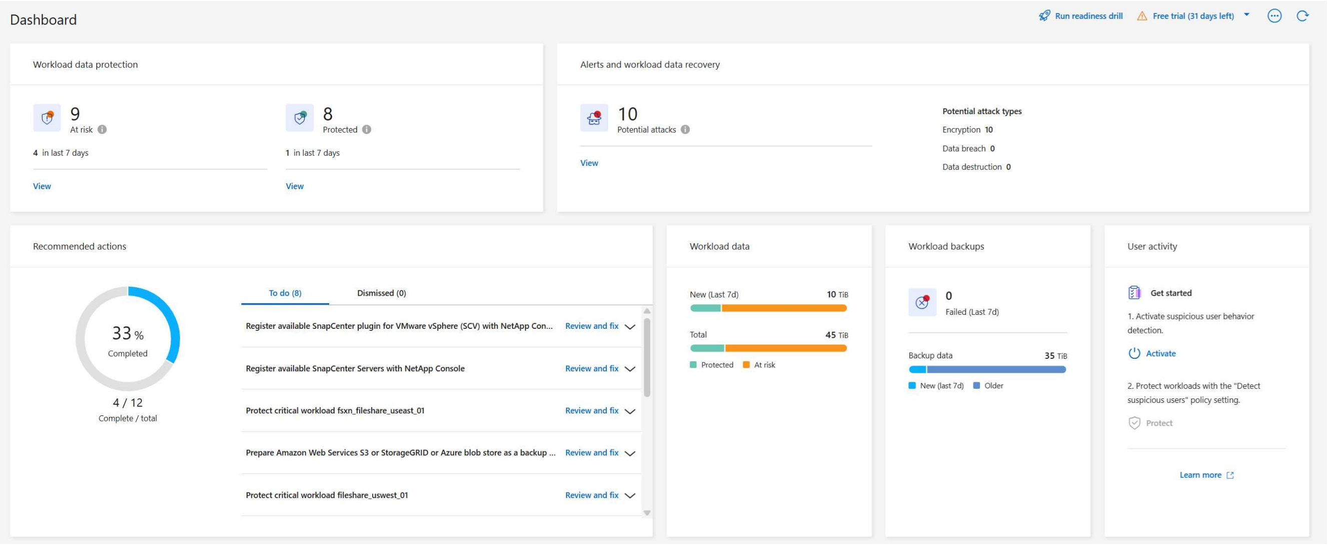
Detect and respond

Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point ⓘ

Recover

Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

Otherwise, the Ransomware Resilience dashboard appears.



Dashboard

Run readiness drill | Free trial (31 days left)

Workload data protection

9 At risk ⓘ — **4** in last 7 days — View

8 Protected ⓘ — **1** in last 7 days — View

Alerts and workload data recovery

10 Potential attacks ⓘ — View

Potential attack types

Encryption **10**

Data breach **0**

Data destruction **0**

Recommended actions

33 % Completed

4 / 12 Complete / total

To do (8) | Dismissed (0)

- Register available SnapCenter plugin for VMware vSphere (SCV) with NetApp Con... — Review and fix
- Register available SnapCenter Servers with NetApp Console — Review and fix
- Protect critical workload fsxn_fileshare_useast_01 — Review and fix
- Prepare Amazon Web Services S3 or StorageGRID or Azure blob store as a backup ... — Review and fix
- Protect critical workload fileshare_uswest_01 — Review and fix

Workload data

New (Last 7d) **10** TiB

Total **45** TiB

🟩 Protected 🟧 At risk

Workload backups

0 Failed (Last 7d)

Backup data **35** TiB

🟦 New (last 7d) 🟦 Older

User activity

Get started

1. Activate suspicious user behavior detection.

Activate

2. Protect workloads with the "Detect suspicious users" policy setting.

Protect

Learn more

4. If you haven’t done so already, select the **Discover Workloads** option.

   Refer to Discover Workloads.

Set up licensing for NetApp Ransomware Resilience

With NetApp Ransomware Resilience, you can use different licensing plans.

To perform this task, you need the Organization admin, Folder or project admin role. Learn about Console access roles.

License types

Ransomware Resilience is available with the following license types:

- 30-day free trial
- Purchase a pay-as-you-go (PAYGO) subscription with Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace, or Azure Marketplace
- Bring your own license (BYOL): a NetApp License File (NLF) that you obtain from your NetApp sales rep. You can use the license serial number to get the BYOL activated in the Console.

After you set up your BYOL or purchase a PAYGO subscription, you can see the license in the Licenses and subscriptions section of the Console.

After the free trial ends or the license or subscription expires, you can still:

- View workloads and workload health
- Delete resources such as policies
- Run all scheduled operations created during the trial period or under the license

Other licenses

The Ransomware Resilience license does not include additional NetApp products. However, Ransomware Resilience can integrate with NetApp Backup and Recovery, even if you do not have a separate license for Backup and Recovery.

> ⓘ If you have both Backup and Recovery and Ransomware Resilience, any common data protected by both products will be billed by Ransomware Resilience only.

Try Ransomware Resilience with a 30-day free trial

You can try Ransomware Resilience with a 30-day free trial. You must be a Console Organization administrator to start the free trial.

Storage capacity limits are not enforced during the trial.

You can get a license or subscribe at any time and you will not be charged until the 30-day trial ends. To continue after the 30-day trial, you'll need to purchase a BYOL license or PAYGO subscription.

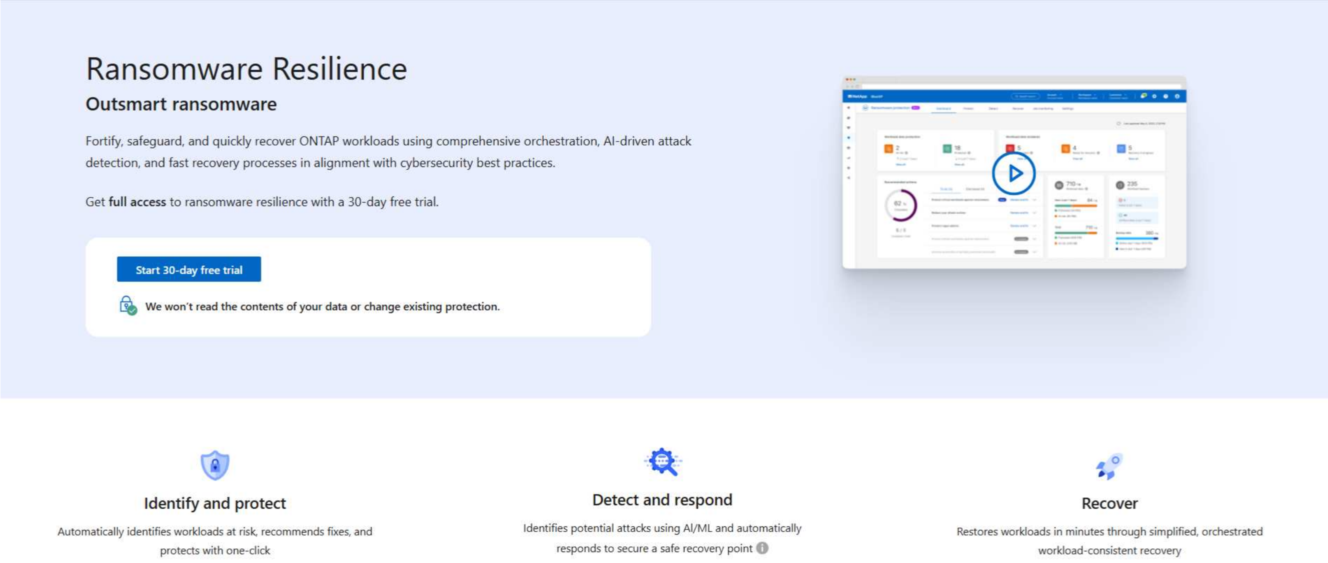
During the trial, you have full functionality.

Steps

1. Access the Console.
2. Log in to the Console.

3. From the NetApp Console, select **Protection** > **Ransomware Resilience**.

   If this is your first time logging in to this service, the landing page appears.



Ransomware Resilience

Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get **full access** to ransomware resilience with a 30-day free trial.

We won't read the contents of your data or change existing protection.

Identify and protect

Automatically identifies workloads at risk, recommends fixes, and protects with one-click

Detect and respond

Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point

Recover

Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

4. If you haven't already added a Console agent for other services, add one.
5. In the Ransomware Resilience landing page, select **Start by discovering workloads** to discover your workloads.

   This option is only available if you've successfully installed a Console agent.

6. To review the free trial information, select the drop-down option in the top right.

After the trial ends, obtain a subscription or license

After the free trial ends, you can either subscribe through one of the Marketplaces or purchase a license from NetApp.

If you already have a PAYGO subscription, the license is automatically switched to the subscription after the free trial ends.

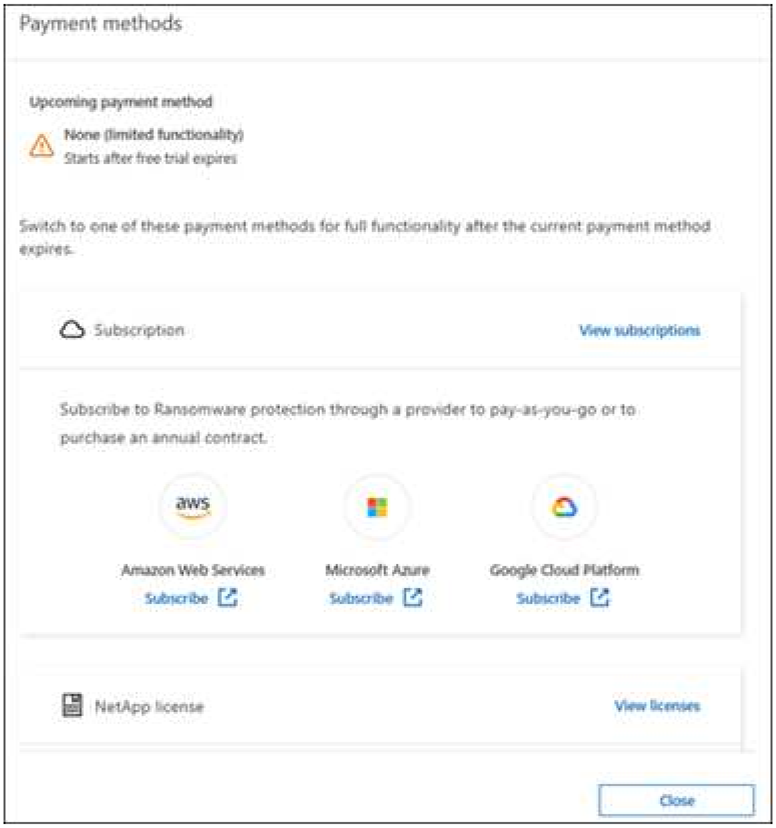
Subscribe through AWS Marketplace
Subscribe through Microsoft Azure Marketplace
Subscribe through Google Cloud Platform Marketplace
Bring your own license (BYOL)

Subscribe through AWS Marketplace

This procedure provides a high level overview of how to subscribe directly in the AWS Marketplace.

Steps

1. In Ransomware Resilience, do one of the following:
   - If you have a message stating free trial is expiring, select **View payment methods**.
   - If you haven't started the trial, select the **Free trial** notice at the top right then **View payment methods**.



Payment methods

Upcoming payment method

None (limited functionality)

Starts after free trial expires

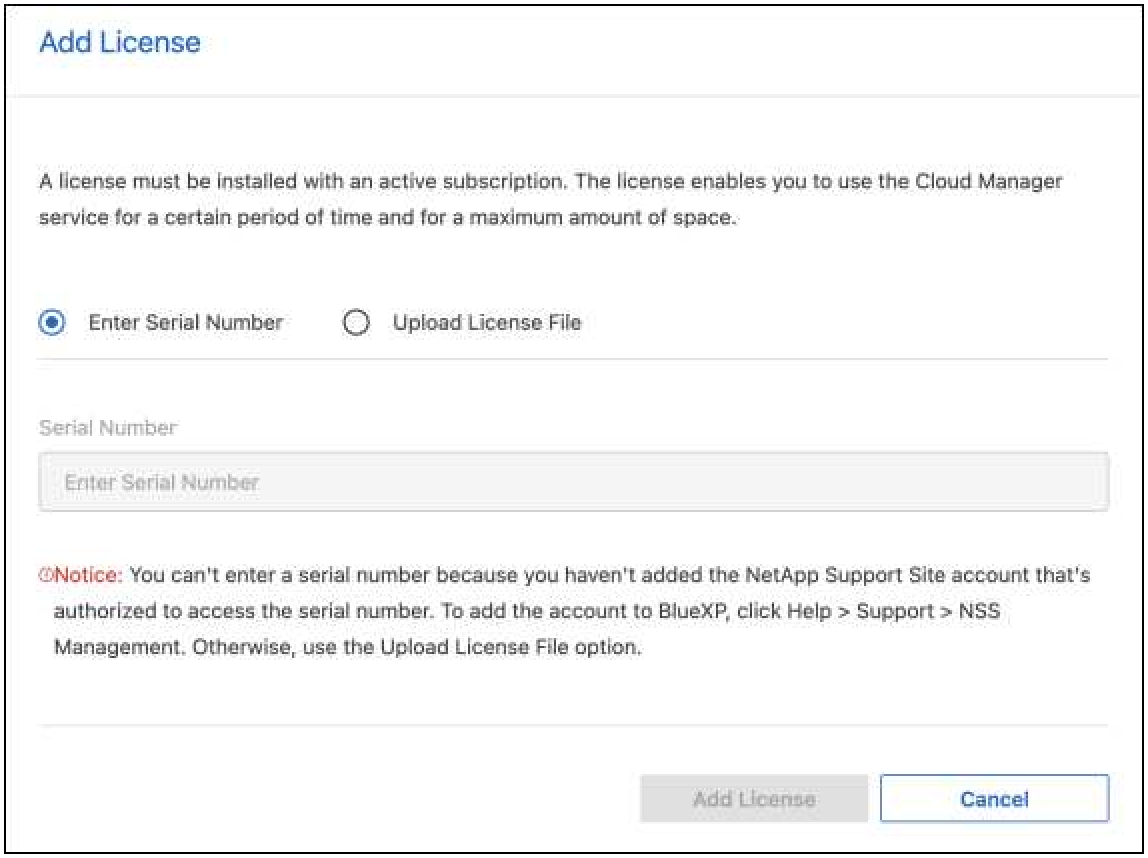
Switch to one of these payment methods for full functionality after the current payment method expires.

Subscribe to Ransomware protection through a provider to pay-as-you-go or to purchase an annual contract.

2. In the Payment methods page, select **Subscribe** for **Amazon Web Services**.
3. In AWS Marketplace, select **View purchase options**.
4. Use AWS Marketplace to subscribe to **NetApp Intelligent Services** and **Ransomware Resilience**.
5. When you return to Ransomware Resilience, a message states that you are subscribed.

> ⓘ An email is sent to you that includes the Ransomware Resilience serial number, and indicates that Ransomware Resilience is subscribed in AWS Marketplace.

6. Return to the Ransomware Resilience payment methods page.
7. Add the license to the Console by selecting **Add license**.



Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

● Enter Serial Number ○ Upload License File

Serial Number

Enter Serial Number

Notice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

8. In the Add License page, select **Enter Serial Number**, enter the serial number that was included in the email sent to you, then select **Add License**.
9. To view license details, from the Console left navigation, select **Administration** > **Licenses and subscriptions**.
   - To see subscription information, select **Subscriptions**.
   - To see BYOL licenses, select **Data Services Licenses**.
10. Return to Ransomware Resilience. From the Console left navigation, select **Protection** > **Ransomware Resilience**.

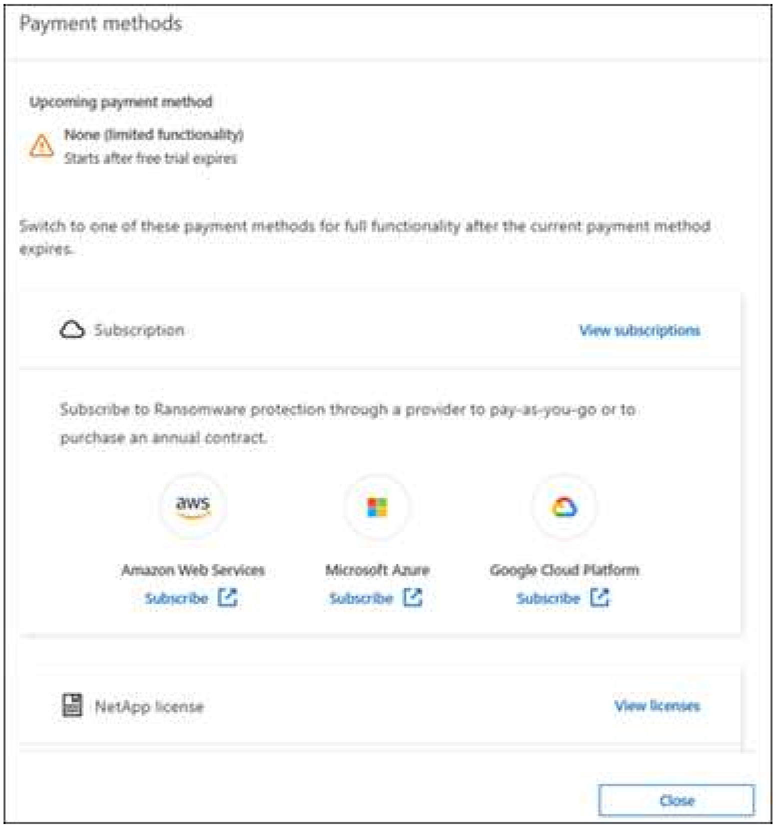
    A message confirms a license has been added.

Subscribe through Microsoft Azure Marketplace

This procedure provides a high level overview of how to subscribe directly in the Azure Marketplace.

Steps

1. In Ransomware Resilience, do one of the following:
   - If you have a message stating free trial is expiring, select **View payment methods**.
   - If you haven’t started the trial, select the **Free trial** notice at the top right then **View payment methods**.



Payment methods

Upcoming payment method

⚠ None (limited functionality)
Starts after free trial expires

Switch to one of these payment methods for full functionality after the current payment method expires.

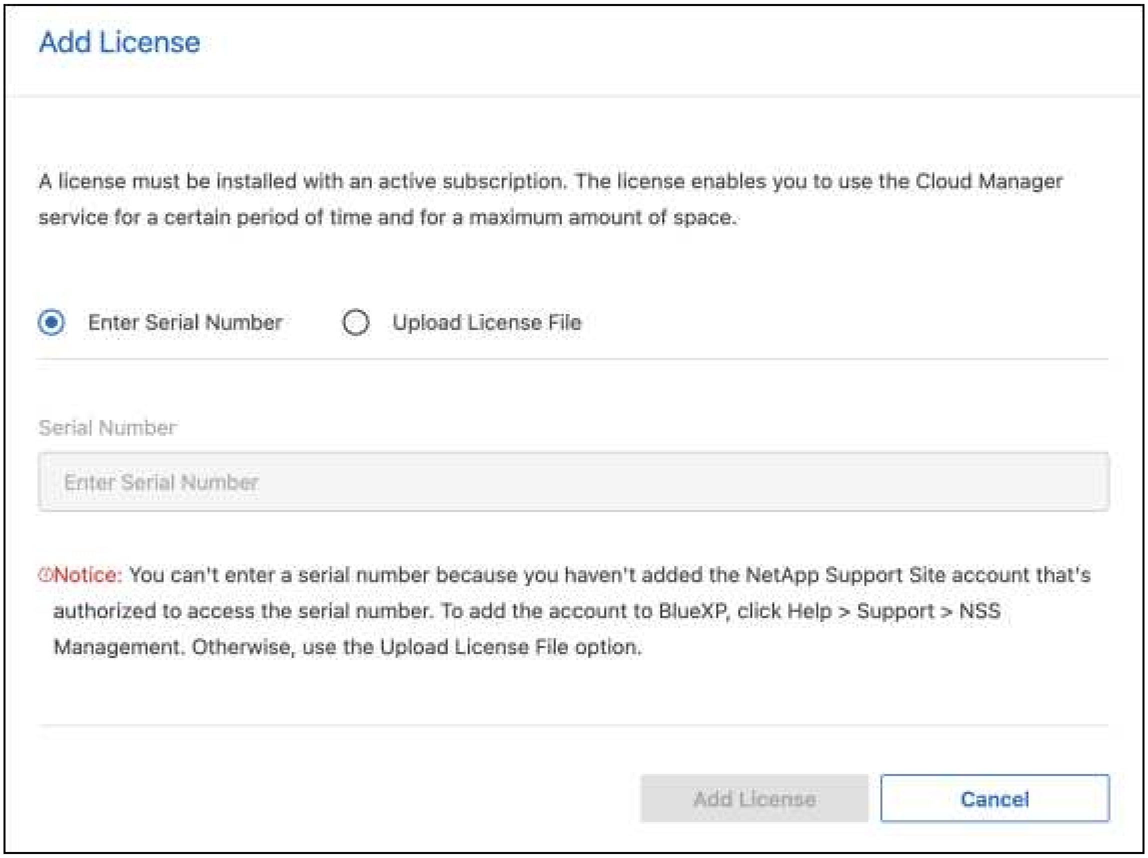
Subscription

Subscribe to Ransomware protection through a provider to pay-as-you-go or to purchase an annual contract.

2. In the Payment methods page, select **Subscribe** for **Microsoft Azure Marketplace**.
3. In Azure Marketplace, select **View purchase options**.
4. Use Azure Marketplace to subscribe to **NetApp Intelligent Services** and **Ransomware Resilience**.
5. When you return to Ransomware Resilience, a message states that you are subscribed.

   An email is sent to you that includes the Ransomware Resilience serial number, and indicates that Ransomware Resilience is subscribed in Azure Marketplace.

6. Return to Ransomware Resilience Payment methods page.
7. To add the license, select **Add a license**.



Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

● Enter Serial Number ○ Upload License File

Serial Number

Enter Serial Number

ⓘNotice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

8. In the Add License page, select **Enter Serial Number** then enter the serial number frin the email sent to you. Select **Add License**.
9. To view license details in Licenses and subscriptions, from the Console left navigation, select **Governance** > **Licenses and subscriptions**.
   - To see subscription information, select **Subscriptions**.
   - To see BYOL licenses, select **Data Services Licenses**.
10. Return to Ransomware Resilience. From the Console left navigation, select **Protection** > **Ransomware Resilience**.

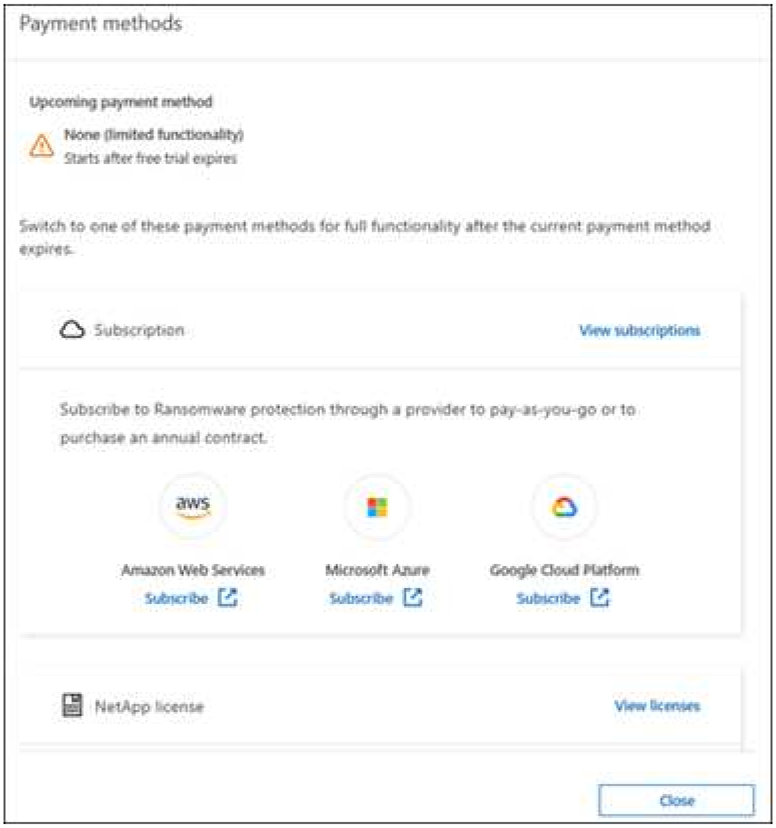
    A message appears indicating that a license has been added.

Subscribe through Google Cloud Platform Marketplace

This procedure provides a high level overview of how to subscribe directly in the Google Cloud Platform Marketplace.

Steps

1. In the Ransomware Resilience, do one of the following:
   - If you have a message stating free trial is expiring, select **View payment methods**.
   - If you haven’t started the trial, select the **Free trial** notice at the top right then **View payment methods**.



Payment methods

Upcoming payment method

None (limited functionality)
Starts after free trial expires

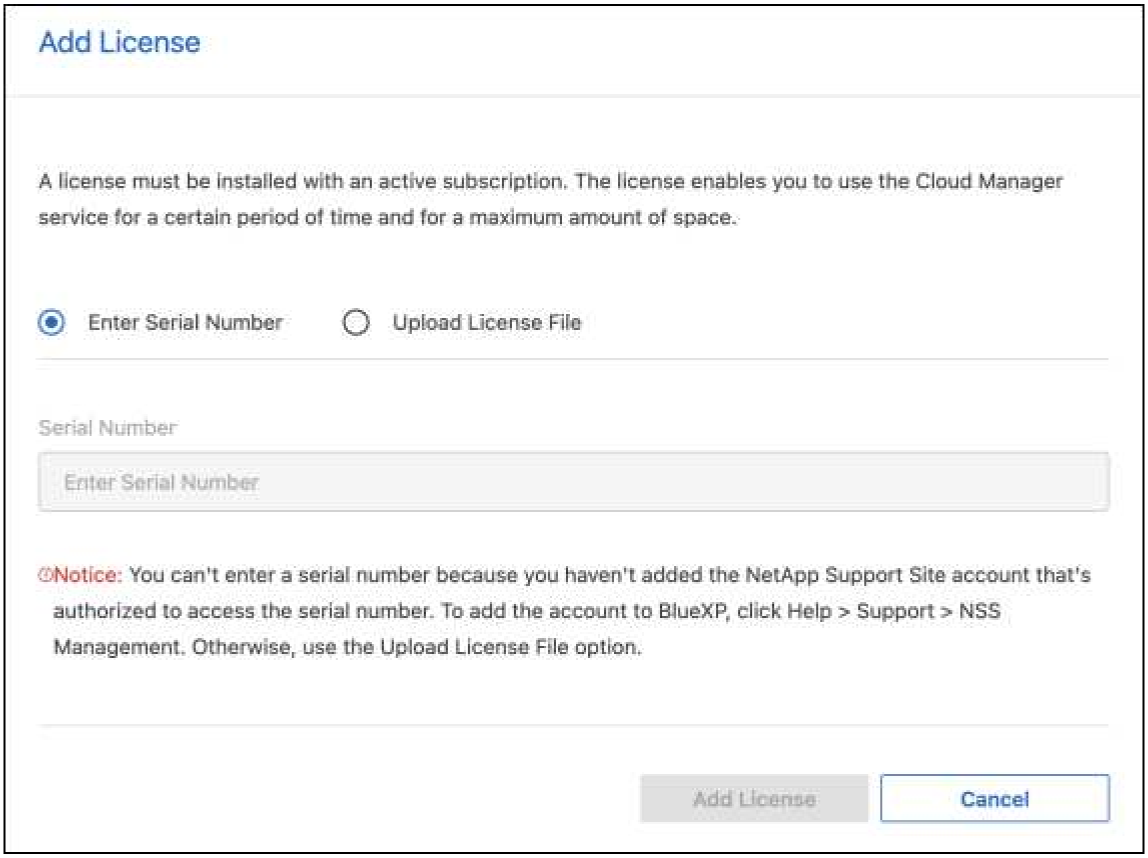
Switch to one of these payment methods for full functionality after the current payment method expires.

Subscribe to Ransomware protection through a provider to pay-as-you-go or to purchase an annual contract.

2. In the Payment methods page, select **Subscribe** for Google Cloud Platform Marketplace*.
3. In Google Cloud Platform Marketplace, select **Subscribe**.
4. Use Google Cloud Platform Marketplace to subscribe to **NetApp Intelligent Services** and **Ransomware Resilience**.
5. When you return to Ransomware Resilience, a message states that you are subscribed.

   > An email is sent to you that includes the Ransomware Resilience serial number and indicates that Ransomware Resilience is subscribed in Google Cloud Platform Marketplace.

6. Return to Ransomware Resilience Payment methods page.
7. To add the license to the Console, select **Add license**.



Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

● Enter Serial Number ○ Upload License File

Serial Number

Enter Serial Number

Notice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

8. In the Add License page, select **Enter Serial Number**. Enter the serial number in the email sent to you. Select **Add License**.
9. To view license details, from the Console left navigation, select **Governance** > **Licenses and subscriptions**.
   - To see subscription information, select **Subscriptions**.
   - To see BYOL licenses, select **Data Services Licenses**.
10. Return to Ransomware Resilience. From the Console left navigation, select **Protection** > **Ransomware Resilience**.

    A message appears indicating that a license has been added.

Bring your own license (BYOL)

If you want to bring your own license (BYOL), you need to purchase the license, get the NetApp License File (NLF), then add the license to the Console.

Add your license file to the Console

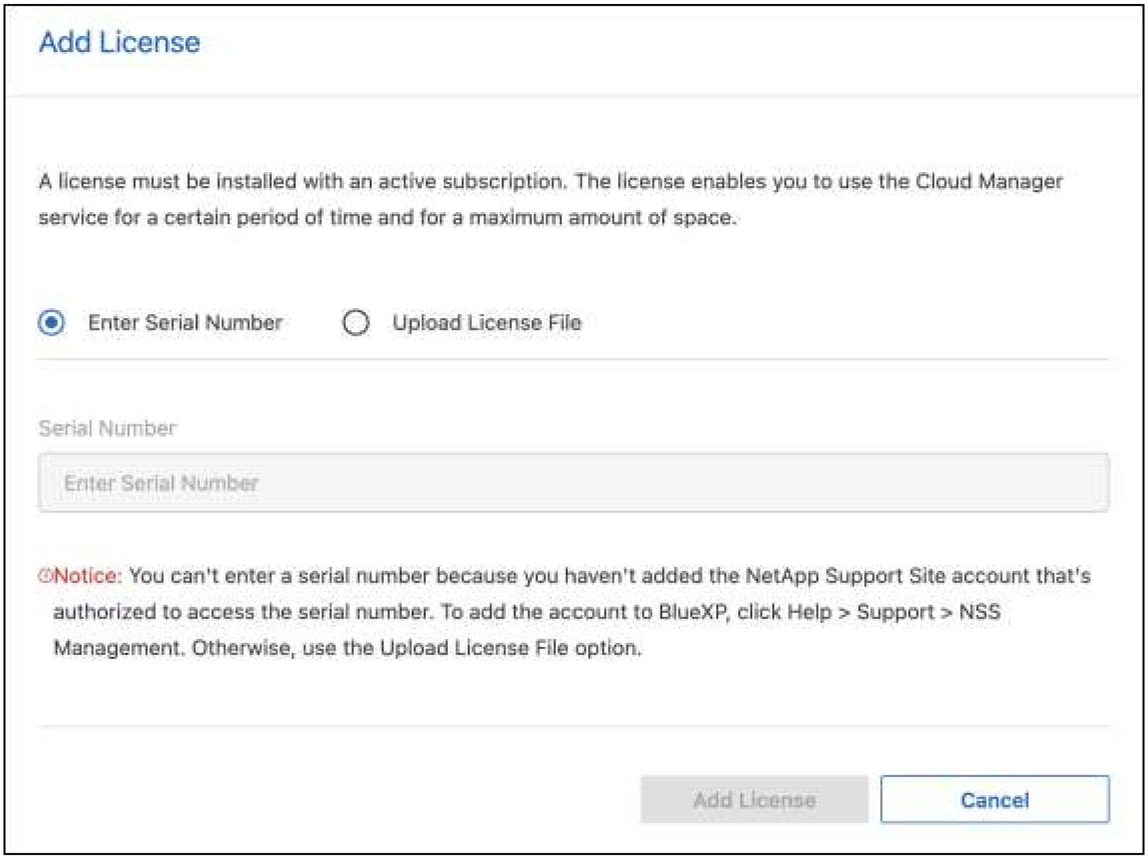
After you’ve purchased your Ransomware Resilience license from your NetApp sales rep, you activate the license by entering the Ransomware Resilience serial number and NetApp Support Site (NSS) account information.

Before you begin

You need the Ransomware Resilience serial number. Locate this number from your sales order, or contact the account team for this information.

Steps

1. After you obtain the license, return to Ransomware Resilience. Select the **View payment methods** option in the upper right. Or, in the message that the free trial is expiring, select **Subscribe or purchase a license**.
2. Select **Add license** to go to the Console Licesnses and subscriptions page.
3. From the **Data Services Licenses** tab, select **Add license**.



Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

● Enter Serial Number ○ Upload License File

Serial Number

Enter Serial Number

ⓘNotice: You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

4. In the Add License page, enter the serial number and NetApp Support Site account information.
   - If you have the Console license serial number and know your NSS account, select the **Enter Serial Number** option and enter that information.

     If your NetApp Support Site account isn't available from the drop-down list, add the NSS account to the Console.
   - If you have the zvondolr license file (required when installed in a dark site), select the **Upload License File** option and follow the prompts to attach the file.
5. Select **Add License**.

Result

The Licenses and subscriptions page shows Ransomware Resilience has a license.

Update your Console license when it expires

If your licensed term is nearing the expiration date, or if your licensed capacity is reaching the limit, you'll be notified in the Ransomware Resilience UI. You can update your Ransomware Resilience license before it expires so there's no interruption in your ability to access your scanned data.

This message also appears in Licenses and subscriptions and in Notification settings.

Steps

1. You can send an email to support to request an update to your license.

   After you pay for the license and it is registered with the NetApp Support Site, the Console automatically updates the license. The Data Services Licenses page will reflect the change in 5 to 10 minutes.

2. If the Console can't automatically update the license, you need to manually upload the license file.
   a. You can obtain the license file from the NetApp Support Site.
   b. In the Console, select **Administration** > **Licenses and subscriptions**.
   c. Select the **Data Services Licenses** tab, select the **Actions …** icon for the serial number you are updating then select **Update License**.

End the PAYGO subscription

If you want to end your PAYGO subscription, you can do so at any time.

Steps

1. In Ransomware Resilience, at the top right, select the license option.
2. Select **View payment methods**.
3. In the drop-down details, uncheck the box **Use after current payment method expires**.
4. Select **Save**.

Discover workloads in NetApp Ransomware Resilience

Before you can use NetApp Ransomware Resilience, it needs to first discover data. During discovery, Ransomware Resilience analyzes all volumes and files in systems across all Console agents and projects within an organization.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

What does Ransomware Resilience discover?
Ransomware Resilience assesses MySQL applications, Oracle applications, VMware datastores, file shares, and block storage.

Ransomware Resilience does not discover workloads with volumes that use FlexGroup.

Ransomware Resilience discovers and displays both supported and unsupported system configurations in the Dashboard.

Ransomware Resilience checks your current backup protection, snapshot copies, and NetApp Autonomous Ransomware Protection options. It then recommends ways to improve your ransomware protection.

How can you discover workloads?
You can do the following:

- Within each Console agent, select the systems where you want to discover workloads. You might benefit from this feature if you want to protect specific workloads in your environment and not others.
- Discover newly created workloads for previously selected systems.
- Discover new systems.

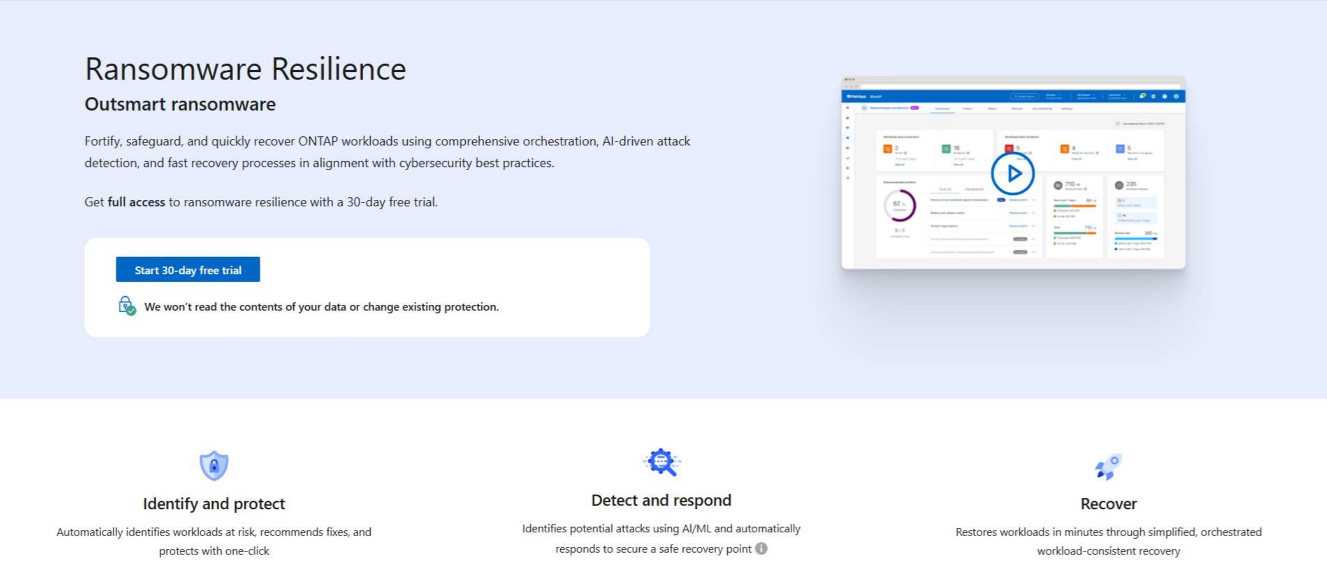
Select workloads to discover and protect

Within each Console agent, select the systems where you want to discover workloads.

Steps

1. From the NetApp Console, select **Protection** > **Ransomware protection**.

   If this is your first login, the landing page appears.

   Ransomware Resilience

   Outsmart ransomware

   Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

   Get **full access** to ransomware resilience with a 30-day free trial.

   Start 30-day free trial

   We won't read the contents of your data or change existing protection.

   Identify and protect

   Automatically identifies workloads at risk, recommends fixes, and protects with one-click

   Detect and respond

   Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point

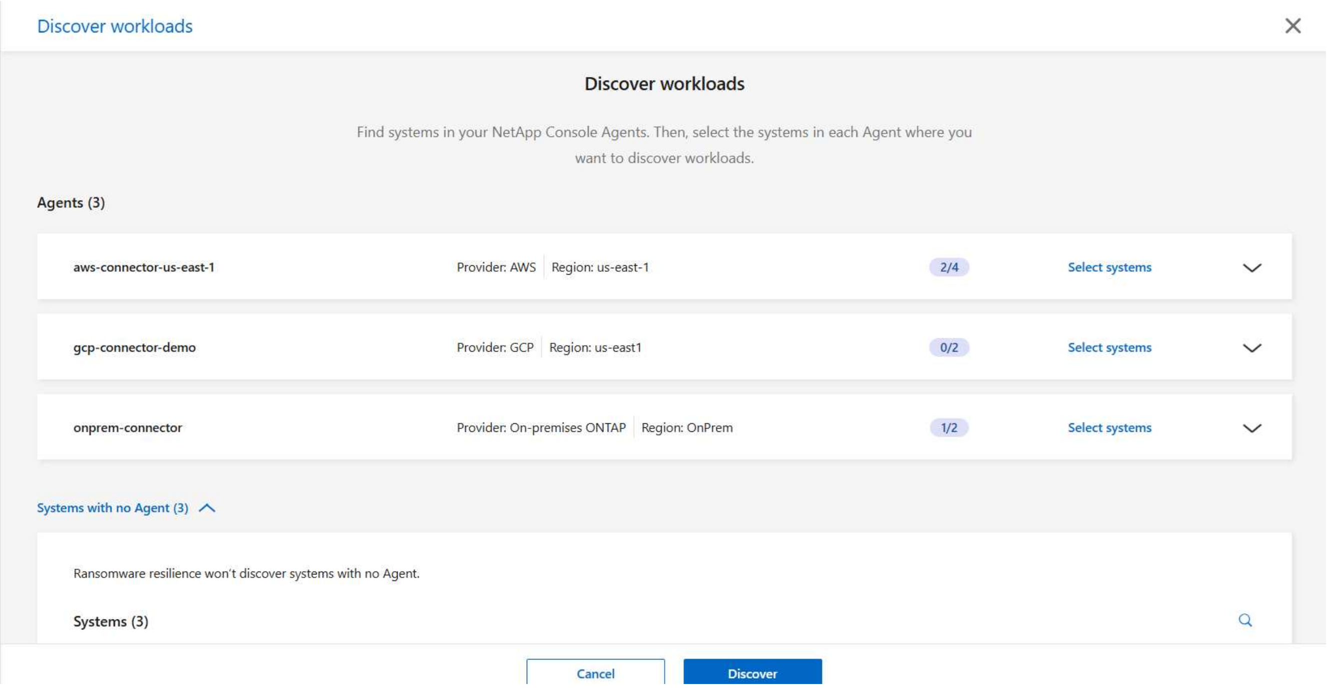
   Recover

   Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

   > If you started the free trial, the **Start 30-day free trial** button label changes to **Start by discovering workloads**.

2. From the initial landing page, select **Start by discovering workloads**.

   Ransomware Resilience finds both supported and unsupported systems. This process might take a few minutes.



Discover workloads

Discover workloads

Find systems in your NetApp Console Agents. Then, select the systems in each Agent where you want to discover workloads.

Agents (3)

aws-connector-us-east-1	Provider: AWS | Region: us-east-1	2/4	Select systems	˅
gcp-connector-demo	Provider: GCP | Region: us-east1	0/2	Select systems	˅
onprem-connector	Provider: On-premises ONTAP | Region: OnPrem	1/2	Select systems	˅

Systems with no Agent (3) ˄

Ransomware resilience won't discover systems with no Agent.

Systems (3)

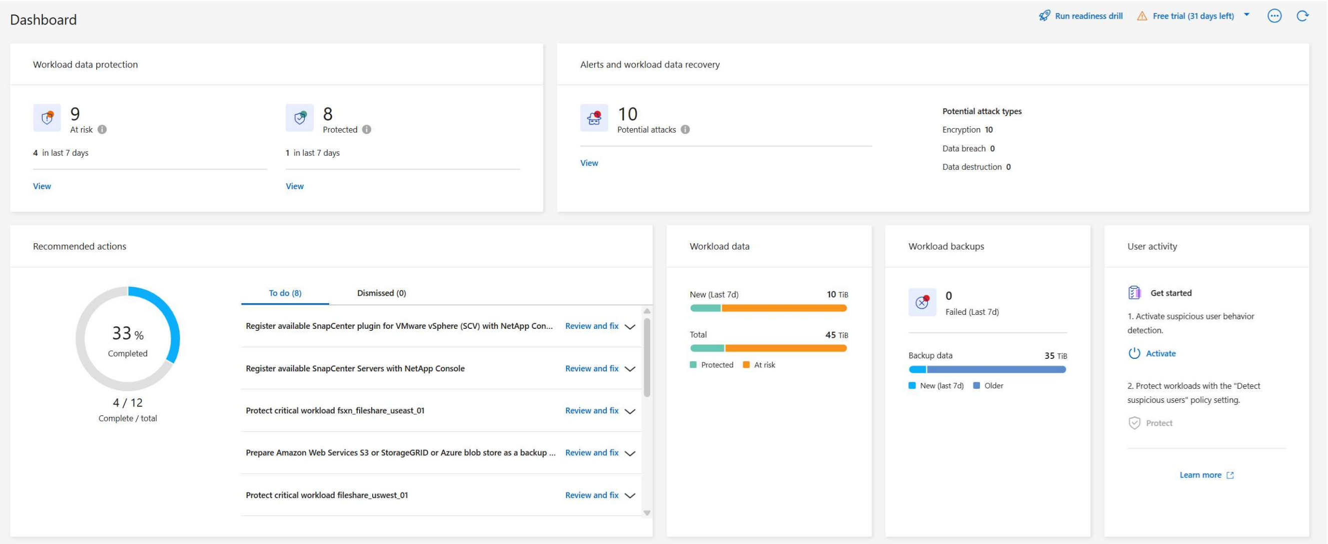
Cancel Discover

3. To discover workloads for a specific Console agent, select **Select systems** next to the Console agent where you want to discover workloads.
4. Select the systems where you want to discover workloads.
5. Select **Discover**.

   Ransomware Resilience discovers workload data only for those Console agents with selected systems. This process might take a few minutes.

6. To download the list of discovered workloads, select **Download results**.
7. To display the Ransomware Resilience dashboard, select **Go to Dashboard**.

   The Dashboard shows data protection health. The number of at-risk or protected workloads updates as new workloads are discovered.



Dashboard

Run readiness drill | Free trial (31 days left)

Workload data protection

9 At risk — 4 in last 7 days — View

8 Protected — 1 in last 7 days — View

Alerts and workload data recovery

10 Potential attacks — View

Potential attack types

Encryption 10

Data breach 0

Data destruction 0

Recommended actions

33 % Completed

4 / 12 Complete / total

To do (8) | Dismissed (0)

Register available SnapCenter plugin for VMware vSphere (SCV) with NetApp Con...	Review and fix
Register available SnapCenter Servers with NetApp Console	Review and fix
Protect critical workload fsxn_fileshare_useast_01	Review and fix
Prepare Amazon Web Services S3 or StorageGRID or Azure blob store as a backup ...	Review and fix
Protect critical workload fileshare_uswest_01	Review and fix

Workload data

New (Last 7d) 10 TiB

Total 45 TiB

Protected | At risk

Workload backups

0 Failed (Last 7d)

Backup data 35 TiB

New (last 7d) | Older

User activity

Get started

1. Activate suspicious user behavior detection.

Activate

2. Protect workloads with the "Detect suspicious users" policy setting.

Protect

Learn more

Learn what the Dashboard shows you.

Discover newly created workloads for previously selected systems

If you have already selected systems for discovery, you can discover newly created workloads for those environments from the Dashboard.

Steps

1. To identify the date of the last discovery, look at the date and time stamp next to **Refresh** icon at the top right of the Ransomware Resilience dashboard.
2. From the Dashboard, select the **Refresh icon** to find new workloads.

Discover new systems

If you have already discovered systems, you can find new or previously unselected ones.

Steps

1. From the Ransomware Resilience menu, select the vertical ⋮ … option at the top right. From the drop-down menu, select **Settings**.
2. In the Workload discovery card, select **Discover workloads**.

   > This process might take a few minutes, and a loading icon shows the progress.

3. Ransomware Resilience discovers both supported and unsupported systems. Ransomware Resilience does not support a system if its ONTAP version is below the required version. When you hover over an unsupported system, a tooltip displays the reason. Select the systems where you want to discover workloads.
4. Select **Discover**.

Conduct a ransomware attack readiness drill in NetApp Ransomware Resilience

Run a ransomware attack readiness drill by simulating an attack on a new sample workload. Investigate the simulated attack and recover the workload. Use this feature to test alert notifications, response, and recovery. Run the drill as often as needed.

> Your real workload data is not impacted.

You can run readiness drills on NFS and CIFS (SMB) workloads.

Configure a ransomware attack readiness drill

Before you run a simulation, set up a drill on the Settings page. Access the Settings page from the Actions option in the top menu.

You need to enter a user name and password for the following situations:

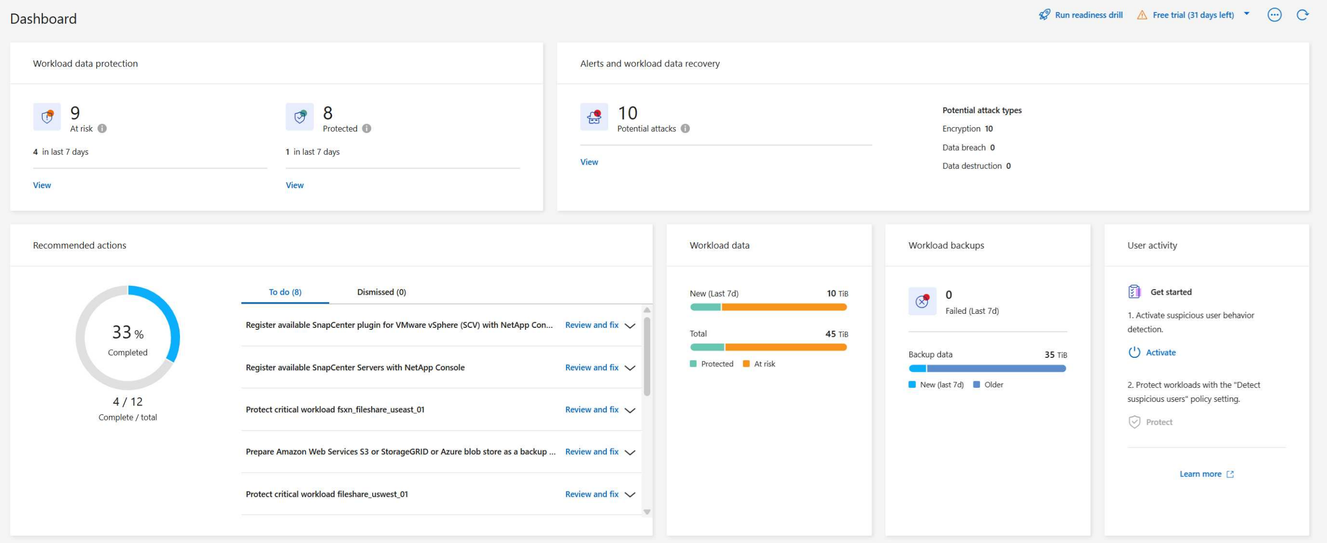
- If user name or password changes occurred for the previously selected storage VM
- If you select a different CIFS (SMB) storage VM

- If you enter a different test workload name

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

Steps

1. From the NetApp Ransomware Resilience menu, select the **Run readiness drill** button at the top right.



Dashboard

Run readiness drill | Free trial (31 days left)

Workload data protection

9 At risk — 4 in last 7 days — View

8 Protected — 1 in last 7 days — View

Alerts and workload data recovery

10 Potential attacks — View

Potential attack types
Encryption 10
Data breach 0
Data destruction 0

Recommended actions

33 % Completed

4 / 12 Complete / total

To do (8) | Dismissed (0)

- Register available SnapCenter plugin for VMware vSphere (SCV) with NetApp Con... — Review and fix
- Register available SnapCenter Servers with NetApp Console — Review and fix
- Protect critical workload fsxn_fileshare_useast_01 — Review and fix
- Prepare Amazon Web Services S3 or StorageGRID or Azure blob store as a backup ... — Review and fix
- Protect critical workload fileshare_uswest_01 — Review and fix

Workload data

New (Last 7d) 10 TiB
Total 45 TiB
Protected | At risk

Workload backups

0 Failed (Last 7d)
Backup data 35 TiB
New (last 7d) | Older

User activity

Get started

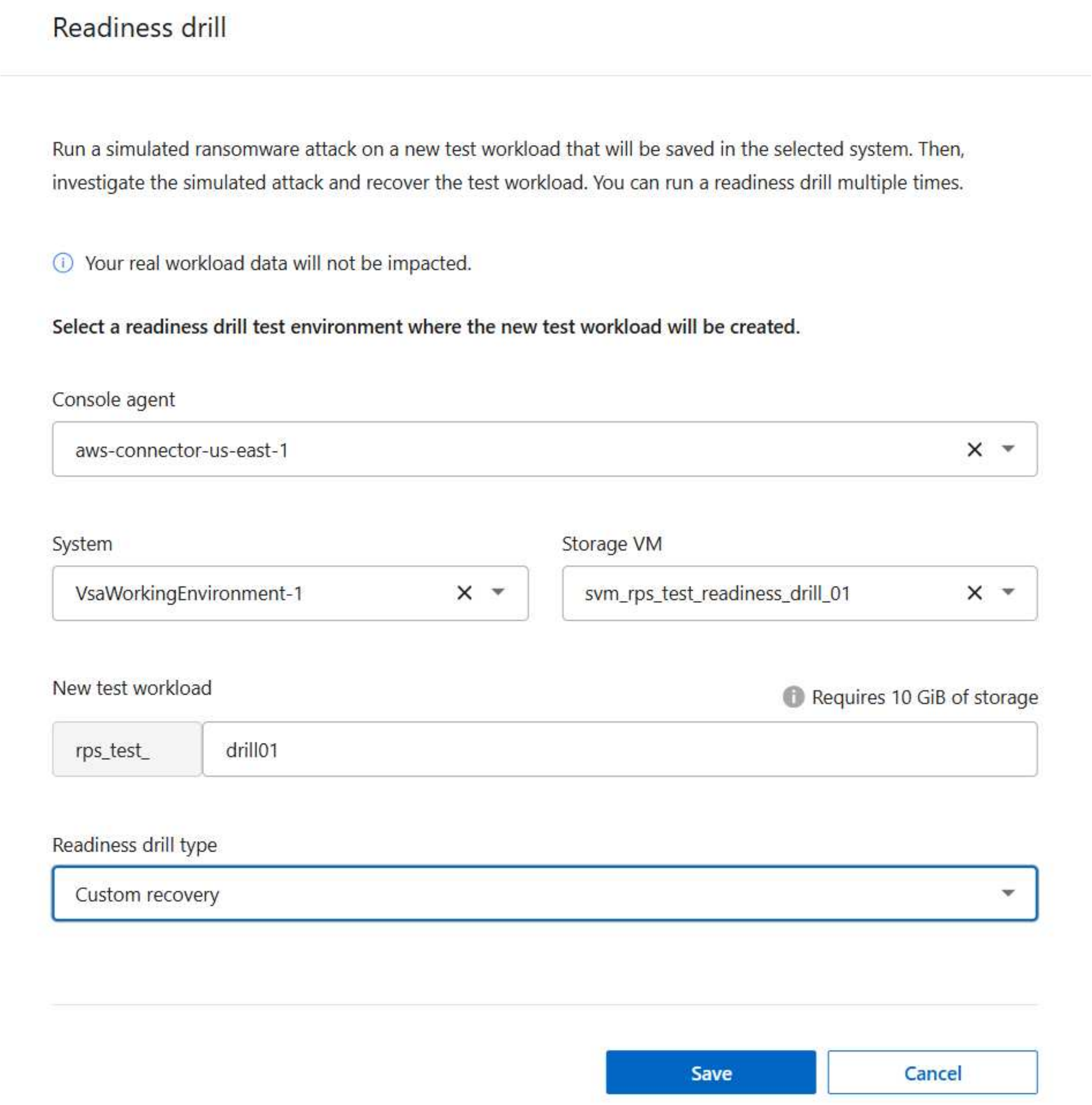
1. Activate suspicious user behavior detection.
Activate

2. Protect workloads with the "Detect suspicious users" policy setting.
Protect

Learn more

2. In the Readiness drill card on the Settings page, select **Configure**.

   The Console displays the Configure readiness drill page.



Readiness drill

Run a simulated ransomware attack on a new test workload that will be saved in the selected system. Then, investigate the simulated attack and recover the test workload. You can run a readiness drill multiple times.

Your real workload data will not be impacted.

Select a readiness drill test environment where the new test workload will be created.

Console agent

aws-connector-us-east-1

System

VsaWorkingEnvironment-1

Storage VM

svm_rps_test_readiness_drill_01

New test workload

rps_test_ drill01

Requires 10 GiB of storage

Readiness drill type

Custom recovery

3. Do the following:
    a. Select the Console agent you want to use for the readiness drill.
    b. Select a test system.
    c. Select a test storage SVM.
    d. If you selected a CIFS (SMB) storage VM, **User name** and **Password** fields appear. Enter the user name and password for the storage VM.
    e. Select the readiness drill type. For a manual recovery from an encryption data breach, choose **Custom recovery**. For recovery from suspicious user activity, choose **Data breach**.
    f. Enter the name of a new test workload to be created. Do not include dashes in the name.

4. Select **Save**.

> You can edit the readiness drill configuration later using the Settings page.

Start a readiness drill

After you configure the readiness drill, you can start the drill.

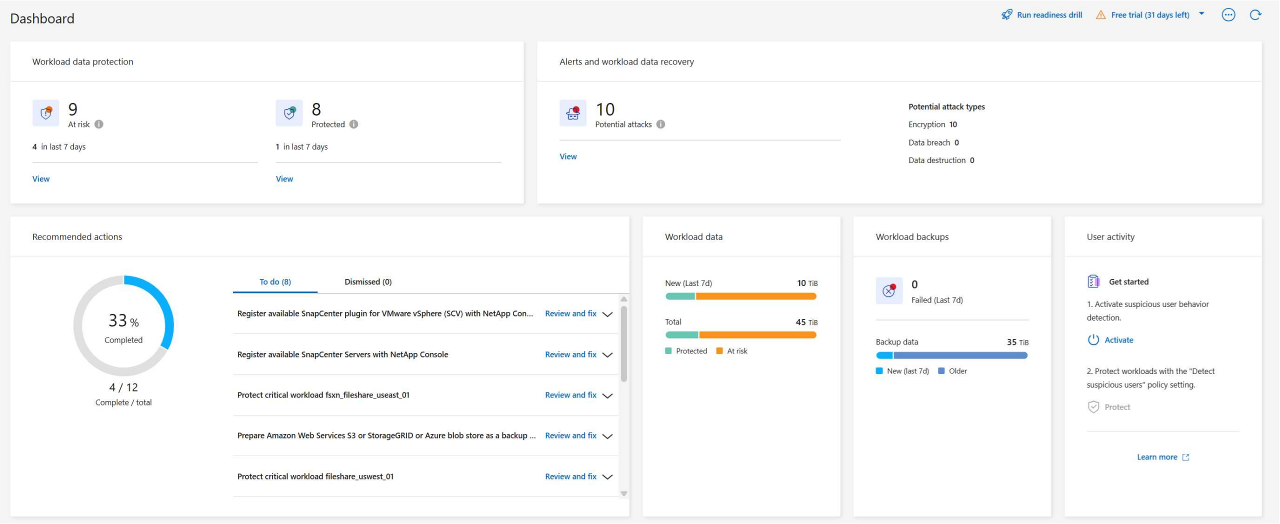
Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

When you start the readiness drill, Ransomware Resilience skips the learning mode and starts the drill in active mode. The detection status of the workload is Active.

> A workload can have a ransomware detection **Learning mode** status when a detection policy is recently assigned and Ransomware Resilience scans workloads.

Steps

1. Do one of the following:
   - From the Ransomware Resilience menu, select the **Run readiness drill** button at the top right.



Register available SnapCenter plugin for VMware vSphere (SCV) with NetApp Con...

Register available SnapCenter Servers with NetApp Console

Protect critical workload fsxn_fileshare_useast_01

Prepare Amazon Web Services S3 or StorageGRID or Azure blob store as a backup ...

Protect critical workload fileshare_uswest_01

1. Activate suspicious user behavior detection.

2. Protect workloads with the "Detect suspicious users" policy setting.

   - OR, from the Settings page, in the Readiness drill card, select **Start**.

> You can’t edit the readiness drill configuration while the drill is running. You can reset the drill to stop it and modify the configuration.

Respond to a readiness drill alert

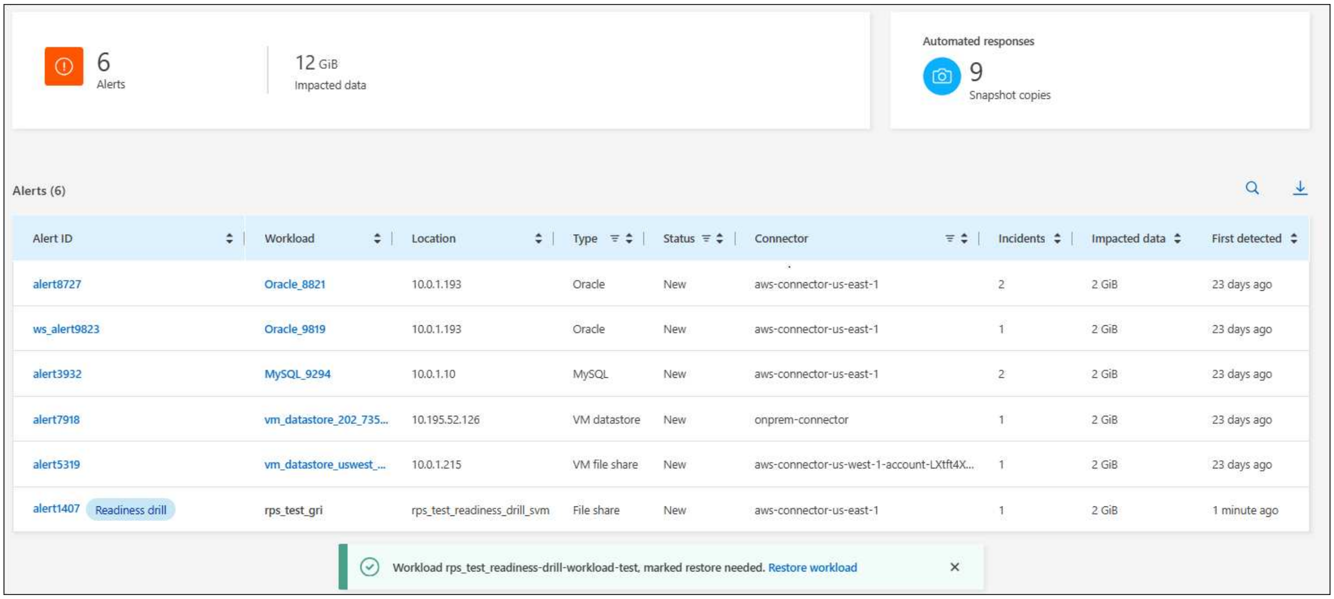
Test your readiness by responding to a readiness drill alert.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

Steps

1. From the Ransomware Resilience menu, select **Alerts**.

   The Console displays the Alerts page. In the Alert ID column, you see "Readiness drill" next to the ID.



6 Alerts

12 GiB Impacted data

Automated responses

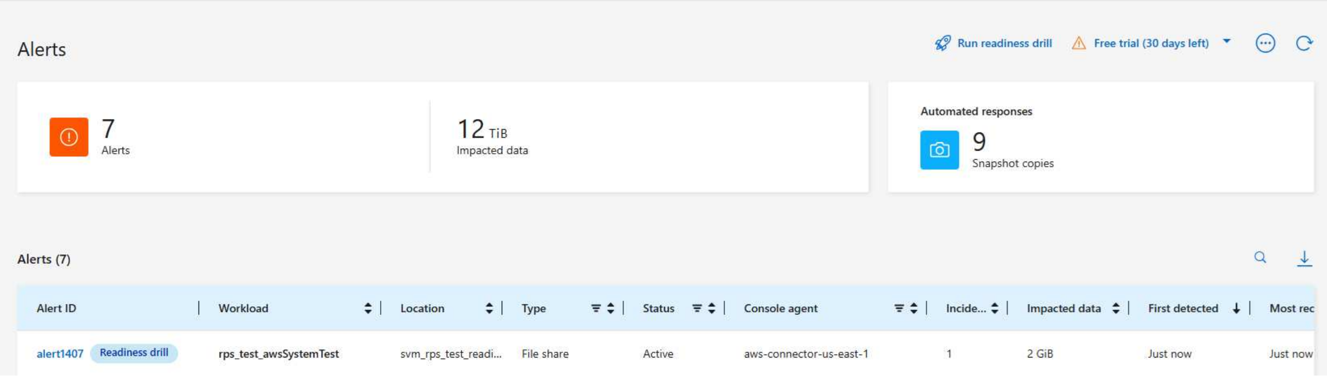
9 Snapshot copies

Alerts (6)

Alert ID	Workload	Location	Type	Status	Connector	Incidents	Impacted data	First detected
alert8727	Oracle_8821	10.0.1.193	Oracle	New	aws-connector-us-east-1	2	2 GiB	23 days ago
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	New	aws-connector-us-east-1	1	2 GiB	23 days ago
alert3932	MySQL_9294	10.0.1.10	MySQL	New	aws-connector-us-east-1	2	2 GiB	23 days ago
alert7918	vm_datastore_202_735...	10.195.52.126	VM datastore	New	onprem-connector	1	2 GiB	23 days ago
alert5319	vm_datastore_uswest_...	10.0.1.215	VM file share	New	aws-connector-us-west-1-account-LXtft4X...	1	2 GiB	23 days ago
alert1407 Readiness drill	rps_test_gri	rps_test_readiness_drill_svm	File share	New	aws-connector-us-east-1	1	2 GiB	1 minute ago

Workload rps_test_readiness-drill-workload-test, marked restore needed. Restore workload

2. Select the alert with the "Readiness drill" indication. A list of incident alerts appears on the Alerts details page.



Alerts

7 Alerts

12 TiB Impacted data

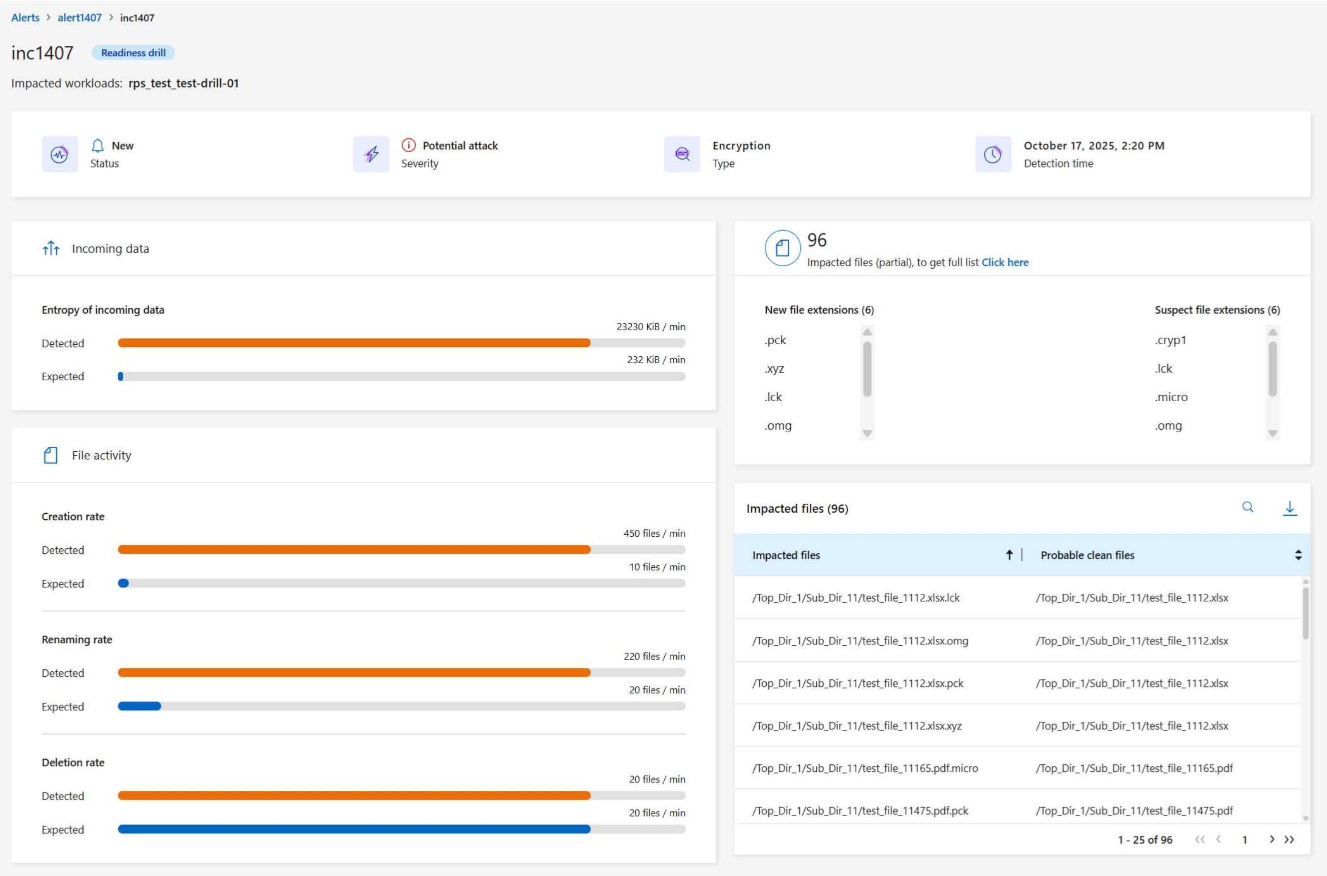
Automated responses

9 Snapshot copies

Alerts (7)

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data	First detected	Most rec
alert1407 Readiness drill	rps_test_awsSystemTest	svm_rps_test_readi...	File share	Active	aws-connector-us-east-1	1	2 GiB	Just now	Just now

3. Review the alert incidents.
4. Select an alert incident.


Alerts > alert1407 > inc1407

inc1407 Readiness drill

Impacted workloads: rps_test_test-drill-01

New
Status

Potential attack
Severity

Encryption
Type

October 17, 2025, 2:20 PM
Detection time

Incoming data

Entropy of incoming data

Detected 23230 KiB / min

Expected 232 KiB / min

File activity

Creation rate

Detected 450 files / min

Expected 10 files / min

Renaming rate

Detected 220 files / min

Expected 20 files / min

Deletion rate

Detected 20 files / min

Expected 20 files / min

96
Impacted files (partial), to get full list Click here

New file extensions (6)	Suspect file extensions (6)
.pck	.cryp1
.xyz	.lck
.lck	.micro
.omg	.omg

Impacted files (96)

Impacted files	Probable clean files
/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx.lck	/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx
/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx.omg	/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx
/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx.pck	/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx
/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx.xyz	/Top_Dir_1/Sub_Dir_11/test_file_1112.xlsx
/Top_Dir_1/Sub_Dir_11/test_file_11165.pdf.micro	/Top_Dir_1/Sub_Dir_11/test_file_11165.pdf
/Top_Dir_1/Sub_Dir_11/test_file_11475.pdf.pck	/Top_Dir_1/Sub_Dir_11/test_file_11475.pdf

1 - 25 of 96 « ‹ 1 › »

Here are some things to look for:

- Look at the Potential attack severity.

  If the severity indicates that a user is suspected of malicious activity, review the user name. You can also block the user.

- Look at the file activity and suspected processes:
  - Look at the incoming detected data compared to the expected data.
  - Look at the creation rate of files that is detected compared to the expected rate.
  - Look at the file renaming rate that is detected compared to the expected rate.
  - Look at the deletion rate compared to the expected rate.
- Look at the list of impacted files. Look at the extensions that might be causing the attack.
- Determine the impact and breadth of the attack by reviewing the number of impacted files and directories.

Restore the test workload

After reviewing the readiness drill alert, restore the test workload if needed.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

Steps

1. Return to the Alert details page.
2. If the test workload should be restored, do the following:
   - Select **Mark restore needed**.
   - Review the confirmation, and select **Mark restore needed** in the confirmation box.
     - From the Ransomware Resilience menu, select **Recovery**.
     - Select the test workload marked with "Readiness drill" that you want to restore.
     - Select **Restore**.
     - In the Restore page, provide information for the restore:
   - Select the source snapshot copy.
   - Select the destination volume.
3. In the restore Review page, select **Restore**.

   The Console displays the status of the Readiness drill restore as "In progress" on the Recovery page.

   After the restore is complete, the Console changes the status of the workload to **Restored**.

4. Review the restored workload.

> For details about the restore process, see Recover from a ransomware attack (after incidents are neutralized).

Change the Alerts status after the readiness drill

After reviewing the readiness drill alert and restoring the workload, change the alert status if needed.

Required the Console role
Organization admin, Folder or project admin, or Ransomware Resilience admin. Learn about Console access roles for all services.

Steps

1. Return to the Alert details page.
2. Select the alert again.
3. Indicate the status by selecting **Edit status** and change the status to one of the following:
   - Dismissed: If you suspect that the activity is not a ransomware attack, change the status to Dismissed.

     > After you dismiss an attack, you cannot chanage it back. If you dismiss a workload, all snapshot copies taken automatically in response to the potential ransomware attack will be permanently deleted. If you dismiss the alert, the readiness drill is considered complete.

   - Resolved: The incident has been mitigated.

Review reports on the readiness drill

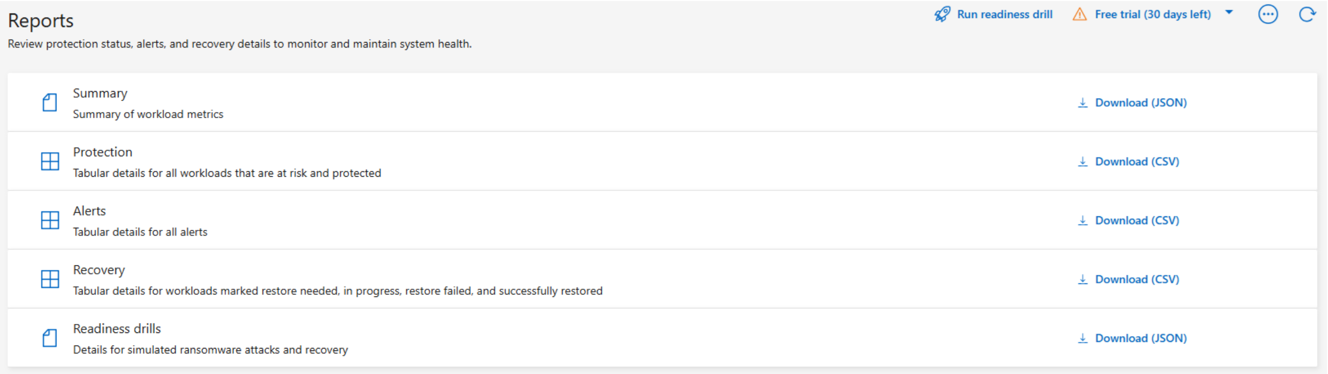
After the readiness drill is complete, you might want to review and save a report on the drill.

Required Console role

To perform this task, you need the Organization admin, Folder or project admin, Ransomware Resilience admin, or Ransomware Resilience viewer role. Learn about Ransomware Resilience roles for NetApp Console.

Steps

1. From the Ransomware Resilience menu, select **Reports**.



Reports

Review protection status, alerts, and recovery details to monitor and maintain system health.

Run readiness drill · Free trial (30 days left)

Summary	Summary of workload metrics	Download (JSON)
Protection	Tabular details for all workloads that are at risk and protected	Download (CSV)
Alerts	Tabular details for all alerts	Download (CSV)
Recovery	Tabular details for workloads marked restore needed, in progress, restore failed, and successfully restored	Download (CSV)
Readiness drills	Details for simulated ransomware attacks and recovery	Download (JSON)

2. Select **Readiness drills** and **Download** to download the readiness drill report.

Configure protection settings in NetApp Ransomware Resilience

You can configure backup destinations, send data to an external security and event management (SIEM) system, conduct an attack readiness drill, configure workload discovery, or configure suspicious user activity detection by accessing the **Settings** option.

Required Console role
To perform this task, you need the Organization admin, Folder or project admin, or Ransomware Resilience admin role. Learn about Ransomware Resilience roles for NetApp Console.

What can you do in the Settings page?
From the Settings page, you can do the following:

- Simulate a ransomware attack by conducting a readiness drill and respond to a simulated ransomware alert. For details, see Conduct a ransomware attack readiness drill.
- Configure workload discovery.
- Configure suspicious user activity reporting.
- Add a backup destination.
- Connect your security and event management system (SIEM) for threat analysis and detection. Enabling threat detection automatically sends data to your SIEM for threat analysis.

Access the Settings page directly

You can easily access the Settings page from the Actions option near the top menu.

1. From the Ransomware Resilience, select the vertical ⋮ … option at the top right.

2. From the drop-down menu, select **Settings**.

Simulate a ransomware attack

Conduct a ransomware readiness drill by simulating a ransomware attack on a newly created, sample workload. Then, investigate the simulated attack and recover the sample workload. This feature helps you know that you are prepared in the event of an actual ransomware attack by testing alert notification, response, and recovery processes. You can run a ransomware readiness drill multiple times.

For details, refer to Conduct a ransomware attack readiness drill.

Configure workload discovery

You can configure workload discovery to automatically discover new workloads in your environment.

1. In the Settings page, locate the **Workload discovery** tile.
2. In the **Workload discovery** tile, select **Discover workloads**.

   This page shows Console agents with systems that were not selected earlier, newly available Console agents, and newly available systems. This page doesn't show those systems that were previously selected.

3. Select the Console agent where you want to discover workloads.
4. Review the list of systems.
5. Check the systems where you want to discover workloads or select the box at the top of the table to discover workloads in all discovered workload environments.
6. Do this for other systems as needed.
7. Select **Discover** to have Ransomware Resilience automatically discover new workloads in the selected Console agent.

Suspicious user activity

In the User activity card, you can create and manage the user activity agent that is required to detect suspicious user activity.

For more information, see Suspicious user activity.

Add a backup destination

Ransomware Resilience can identify workloads that do not have any backups yet and also workloads that do not have any backup destinations assigned yet.

To protect those workloads, you should add a backup destination. You can choose one of the following backup destinations:

- NetApp StorageGRID
- Amazon Web Services (AWS)
- Google Cloud Platform
- Microsoft Azure

Backup destinations are not available for workloads in Amazon FSx for NetApp ONTAP. Perform backup operations using the FSx for ONTAP backup service.

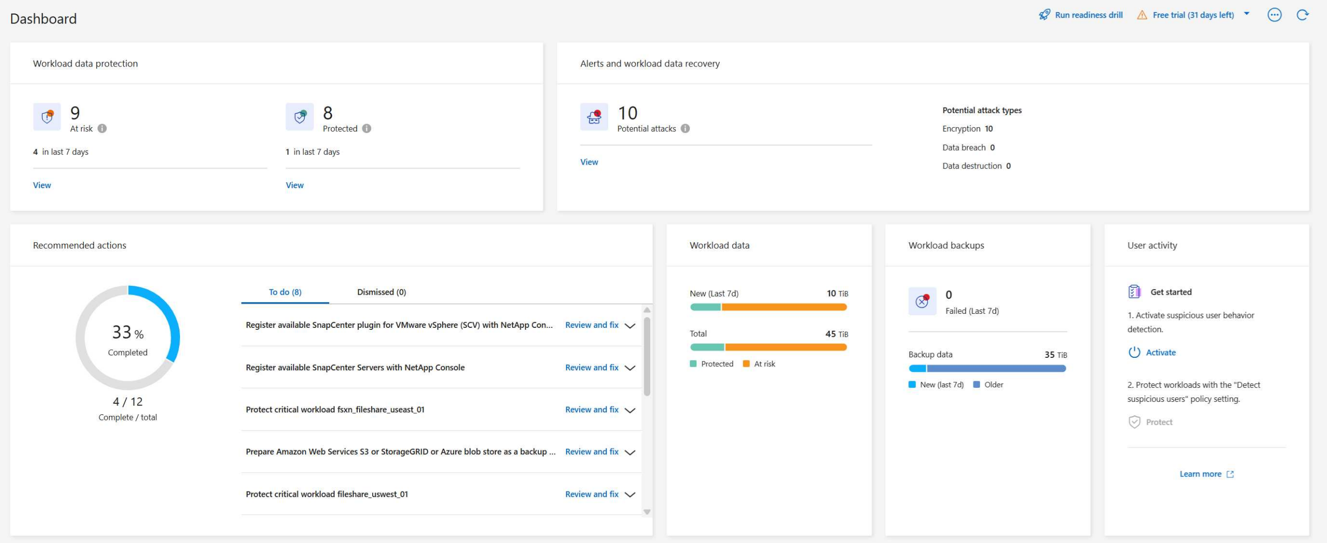
You can add a backup destination based on a recommended action from the Dashboard or from accessing the Settings option on the menu.

Access Backup Destination options from the Dashboard’s recommended actions

The Dashboard provides many recommendations. One recommendation might be to configure a backup destination.

Steps

1. In the Ransomware Resilience dashboard, review the Recommended actions pane.



Register available SnapCenter plugin for VMware vSphere (SCV) with NetApp Con...	Review and fix
Register available SnapCenter Servers with NetApp Console	Review and fix
Protect critical workload fsxn_fileshare_useast_01	Review and fix
Prepare Amazon Web Services S3 or StorageGRID or Azure blob store as a backup ...	Review and fix
Protect critical workload fileshare_uswest_01	Review and fix

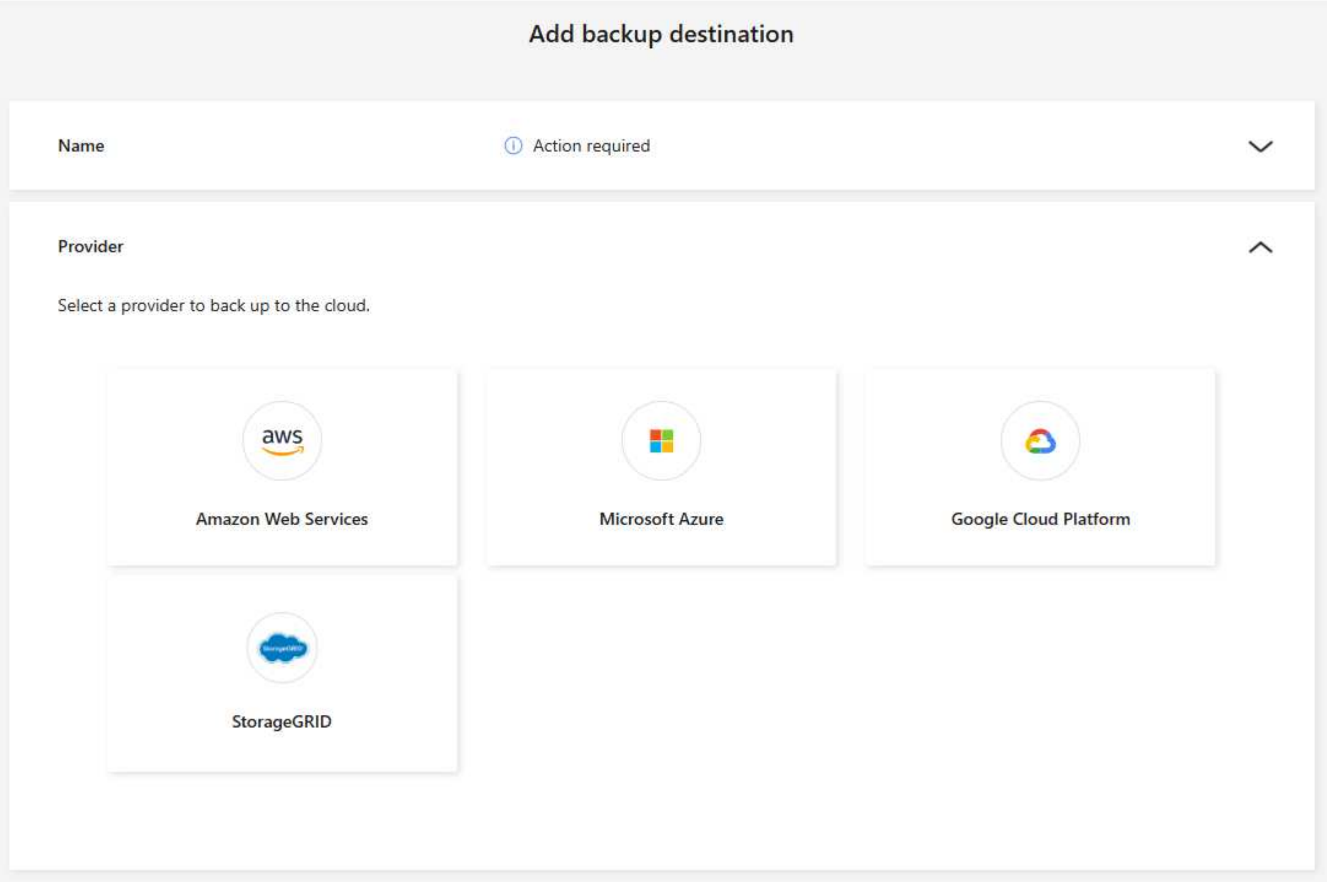
2. From the Dashboard, select **Review and fix** for the recommendation of "Prepare <backup provider> as a backup destination."
3. Continue with instructions depending on the backup provider.

Add StorageGRID as a backup destination

To set up NetApp StorageGRID as a backup destination, enter the following information.

Steps

1. In the **Settings > Backup destinations** page, select **Add**.
2. Enter a name for the backup destination.



Add backup destination

Name ⓘ Action required

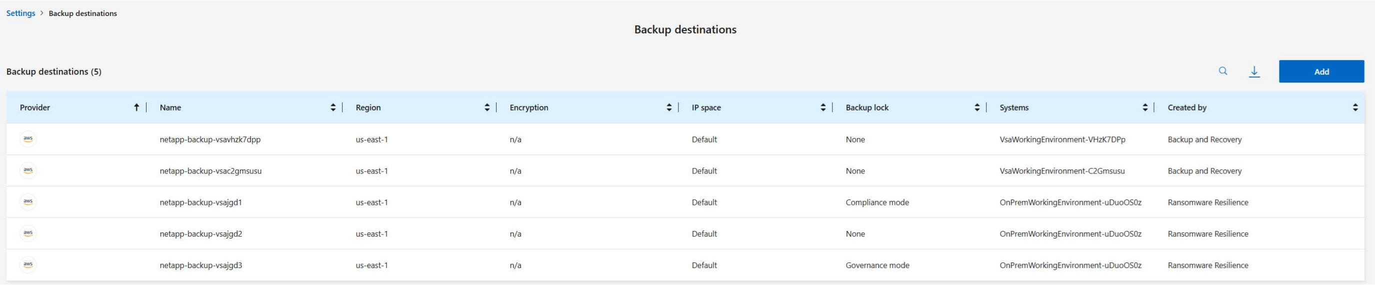
Provider

Select a provider to back up to the cloud.

3. Select **StorageGRID**.
4. Select the down arrow next to each setting and enter or select values:
   - **Provider settings**:
     - Create a new bucket or bring your own bucket that will store the backups.
     - StorageGRID gateway node fully qualified domain name, port, StorageGRID access key and secret key credentials.
   - **Networking**: Choose the IPspace.
     - The IPspace is the cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
5. Select **Add**.

Result

The new backup destination is added to the list of backup destinations.



Backup destinations

Backup destinations (5)

Provider	Name	Region	Encryption	IP space	Backup lock	Systems	Created by
aws	netapp-backup-vsavhzk7dpp	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VHzK7DPp	Backup and Recovery
aws	netapp-backup-vsac2gmsusu	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsusu	Backup and Recovery
aws	netapp-backup-vsajgd1	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuoOS0z	Ransomware Resilience
aws	netapp-backup-vsajgd2	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuoOS0z	Ransomware Resilience
aws	netapp-backup-vsajgd3	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuoOS0z	Ransomware Resilience

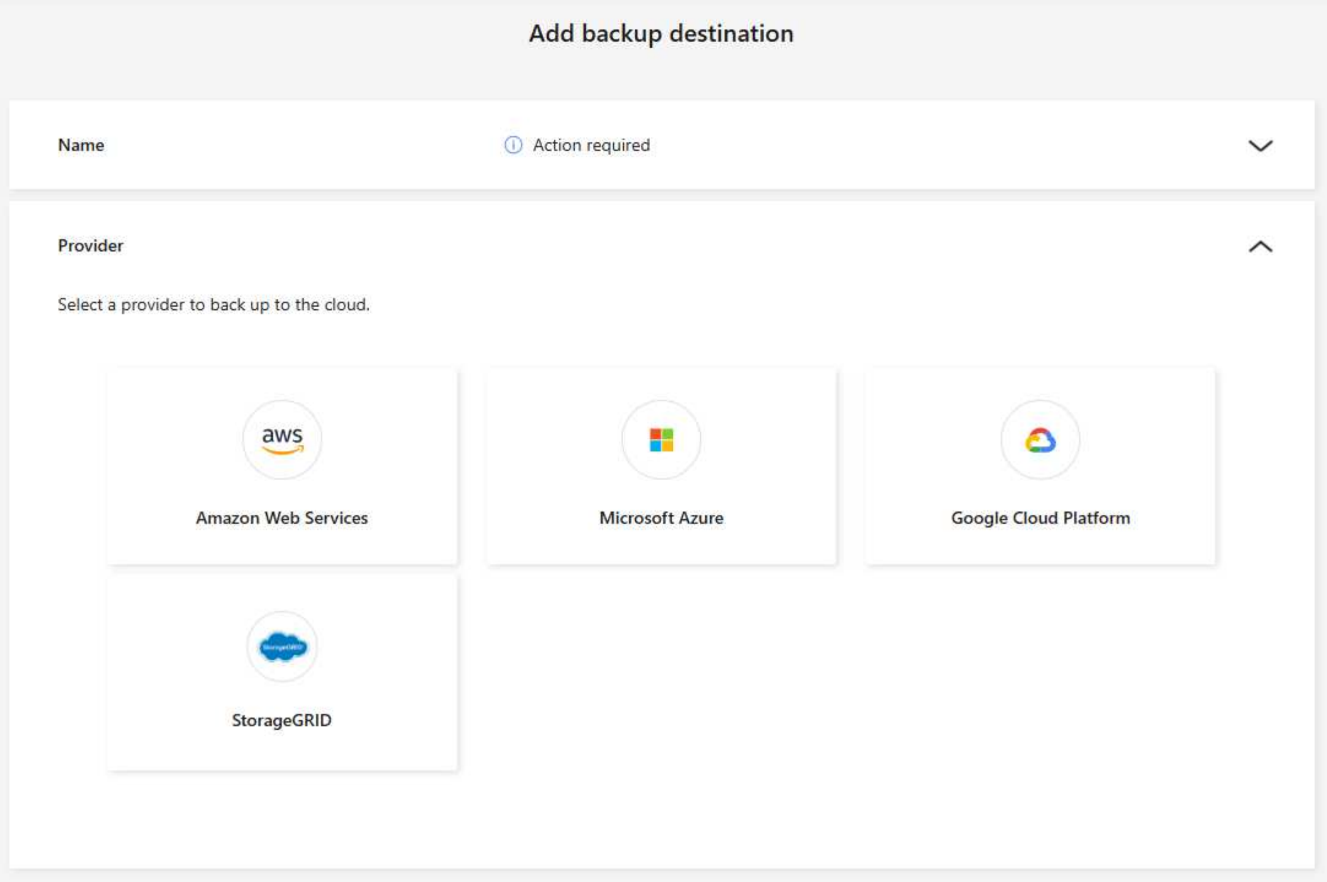
Add Amazon Web Services as a backup destination

To set up AWS as a backup destination, enter the following information.

For details about managing your AWS storage in the Console, refer to Manage your Amazon S3 buckets.

Steps

1. In the **Settings > Backup destinations** page, select **Add**.
2. Enter a name for the backup destination.



Add backup destination

Name — Action required

Provider

Select a provider to back up to the cloud.

3. Select **Amazon Web Services**.
4. Select the Down arrow next to each setting and enter or select values:
    - **Provider settings**:
        - Create a new bucket, select an existing bucket if one already exists in the Console, or bring your own bucket that will store the backups.
        - AWS account, region, access key and secret key for AWS credentials

          If you want to bring your own bucket, refer to Add S3 buckets.
    - **Encryption**: If you are creating a new S3 bucket, enter encryption key information given to you from the provider. If you chose an existing bucket, encryption information is already available.

      Data in the bucket is encrypted with AWS-managed keys by default. You can continue to use AWS-managed keys, or you can manage the encryption of your data using your own keys.
    - **Networking**: Choose the IPspace and whether you'll be using a Private Endpoint.

        - The IPspace is the cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
        - Optionally, choose whether you'll use an AWS private endpoint (PrivateLink) that you previously configured.

          If you want to use AWS PrivateLink, refer to AWS PrivateLink for Amazon S3.

    - **Backup lock**: Choose whether you want Ransomware Resilience to protect backups from being modified or deleted. This option uses the NetApp DataLock technology. Each backup will be locked during the retention period, or for a minimum of 30 days, plus a buffer period of up to 14 days.

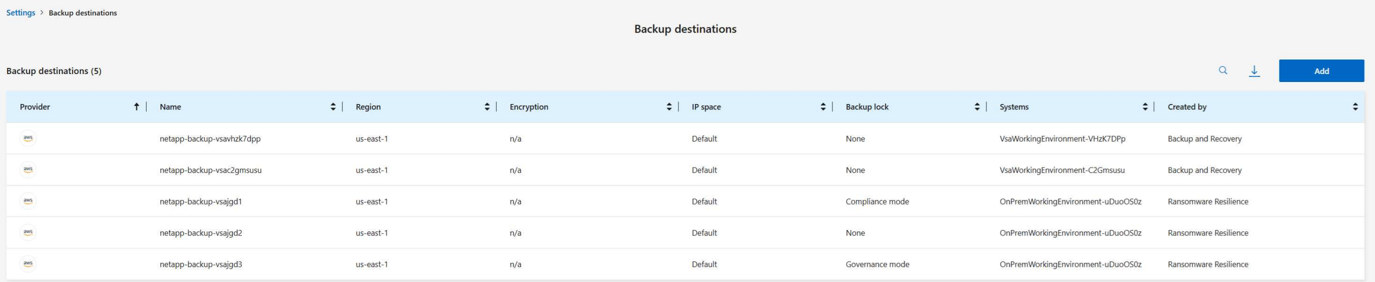
      > ! If you configure the backup lock setting now, you cannot change the setting later after the backup destination is configured.

        - **Governance mode**: Specific users (with s3:BypassGovernanceRetention permission) can overwrite or delete protected files during the retention period.
        - **Compliance mode**: Users cannot overwrite or delete protected backup files during the retention period.

5. Select **Add**.

Result

The new backup destination is added to the list of backup destinations.



Backup destinations

Backup destinations (5)

Provider	Name	Region	Encryption	IP space	Backup lock	Systems	Created by
aws	netapp-backup-vsavhzk7dpp	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VHzK7DPp	Backup and Recovery
aws	netapp-backup-vsac2gmsusu	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsusu	Backup and Recovery
aws	netapp-backup-vsajgd1	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuoOS0z	Ransomware Resilience
aws	netapp-backup-vsajgd2	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuoOS0z	Ransomware Resilience
aws	netapp-backup-vsajgd3	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuoOS0z	Ransomware Resilience

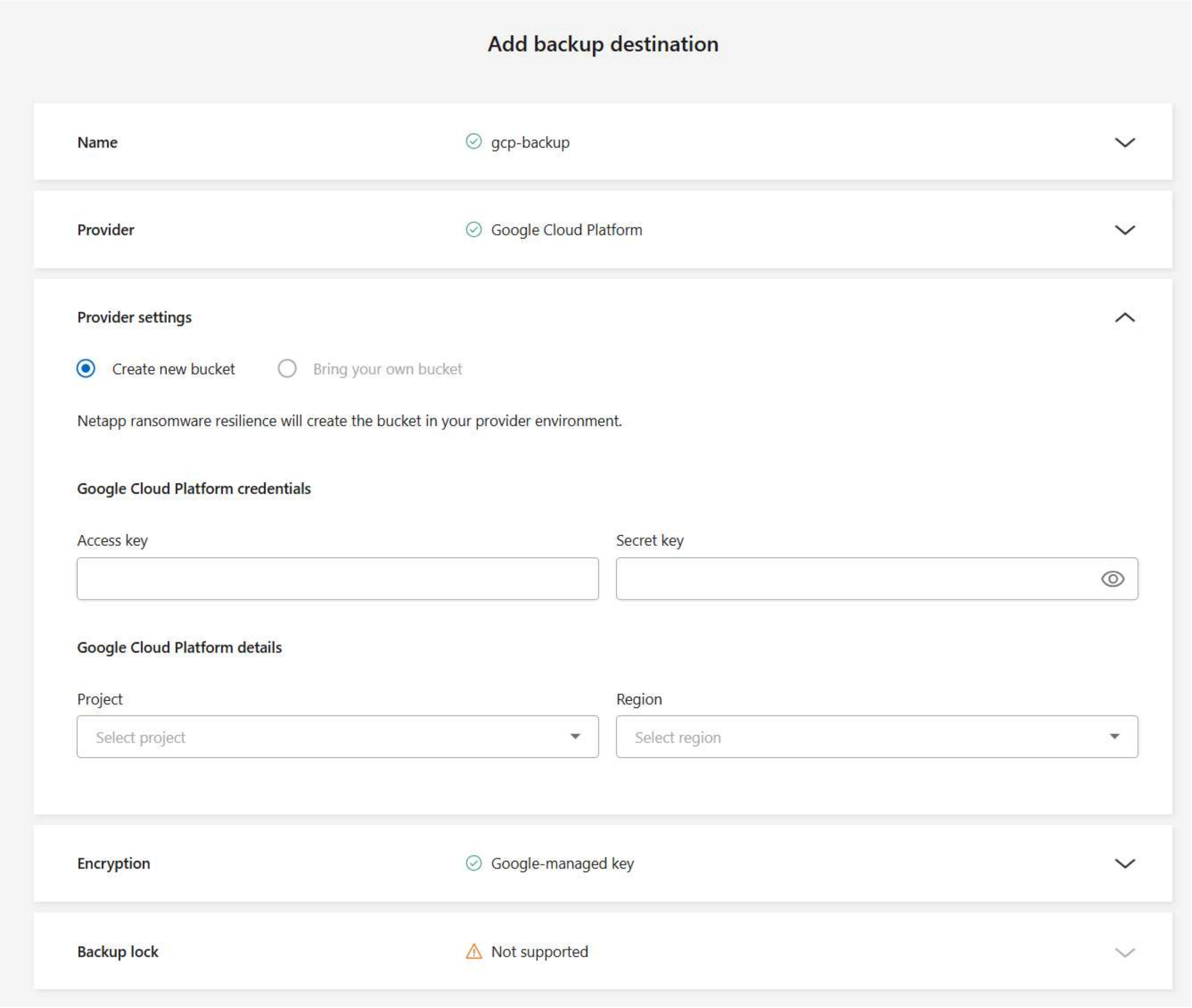
Add Google Cloud Platform as a backup destination

To set up Google Cloud Platform (GCP) as a backup destination, enter the following information.

For details about managing your GCP storage in the Console, refer to Console agent installation options in Google Cloud.

Steps

1. In the **Settings > Backup destinations** page, select **Add**.
2. Enter a name for the backup destination.
3. Select **Google Cloud Platform**.
4. Select the Down arrow next to each setting and enter or select values:
    - **Provider settings**:
        - Create a new bucket. Enter the access key and secret key.
        - Enter or select your Google Cloud Platform project and region.



Add backup destination

Name: gcp-backup

Provider: Google Cloud Platform

Provider settings

● Create new bucket ○ Bring your own bucket

Netapp ransomware resilience will create the bucket in your provider environment.

Google Cloud Platform credentials

Access key:

Secret key:

Google Cloud Platform details

Project: Select project

Region: Select region

Encryption: Google-managed key

Backup lock: Not supported

- **Encryption**: If you are creating a new bucket, enter encryption key information given to you from the provider. If you chose an existing bucket, encryption information is already available.

  Data in the bucket is encrypted with Google-managed keys by default. You can continue to use Google-managed keys.

- **Networking**: Choose the IPspace and whether you'll be using a Private Endpoint.
  - The IPspace is the cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
  - Optionally, choose whether you'll use an GCP private endpoint (PrivateLink) that you previously configured.

5. Select **Add**.

Result

The new backup destination is added to the list of backup destinations.

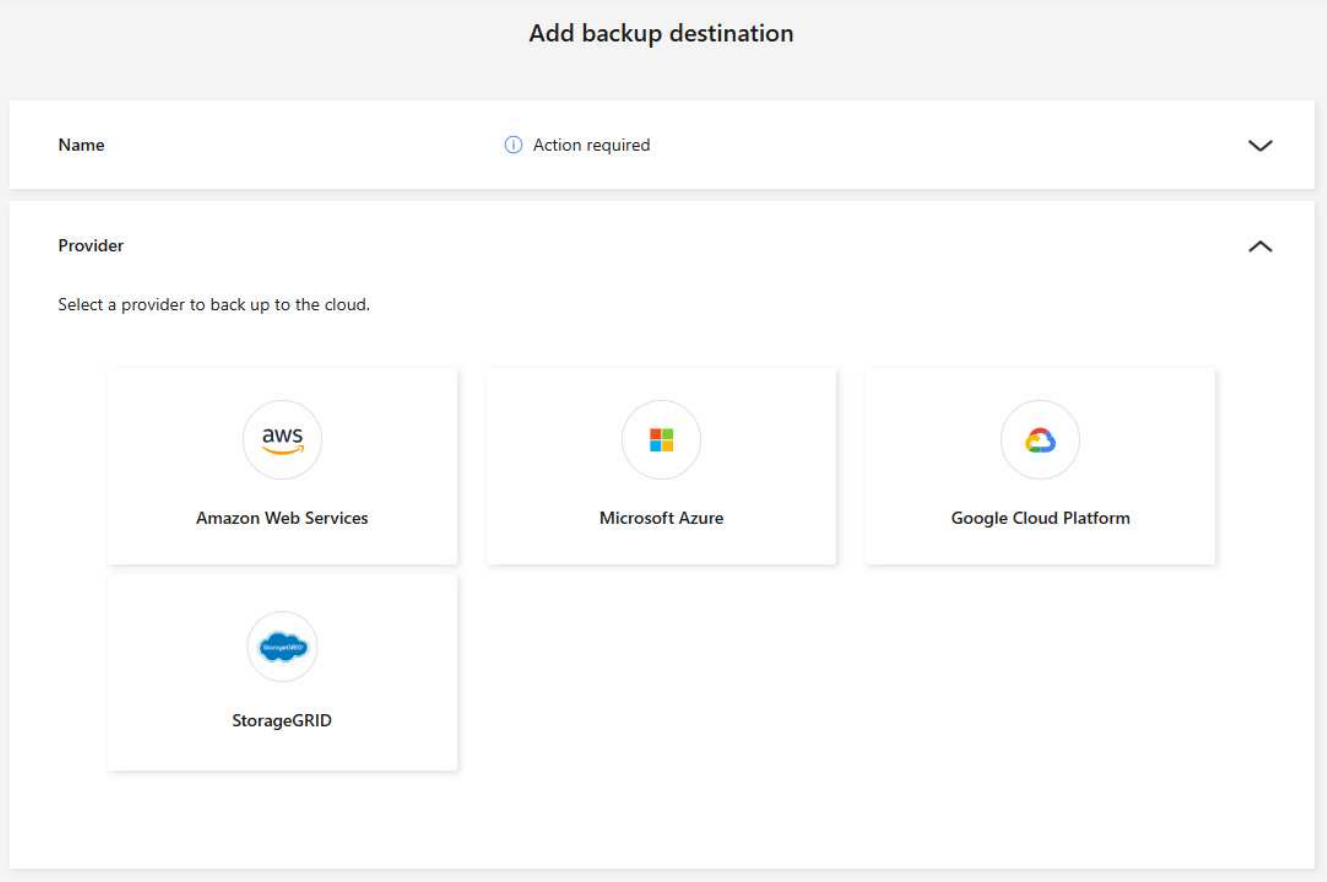
Add Microsoft Azure as a backup destination

To set up Azure as a backup destination, enter the following information.

For details about managing your Azure credentials and marketplace subscriptions in the Console, refer to Manage your Azure credentials and marketplace subscriptions.

Steps

1. In the **Settings > Backup destinations** page, select **Add**.
2. Enter a name for the backup destination.



Add backup destination

Name ⓘ Action required

Provider

Select a provider to back up to the cloud.

3. Select **Azure**.
4. Select the Down arrow next to each setting and enter or select values:
    - **Provider settings**:
        - Create a new storage account, select an existing one if one already exists in the Console, or bring your own storage account that will store the backups.
        - Azure subscription, region, and resource group for Azure credentials

          If you want to bring your own storage account, refer to Add Azure Blob storage accounts.
    - **Encryption**: If you are creating a new storage account, enter encryption key information given to you from the provider. If you chose an existing account, encryption information is already available.

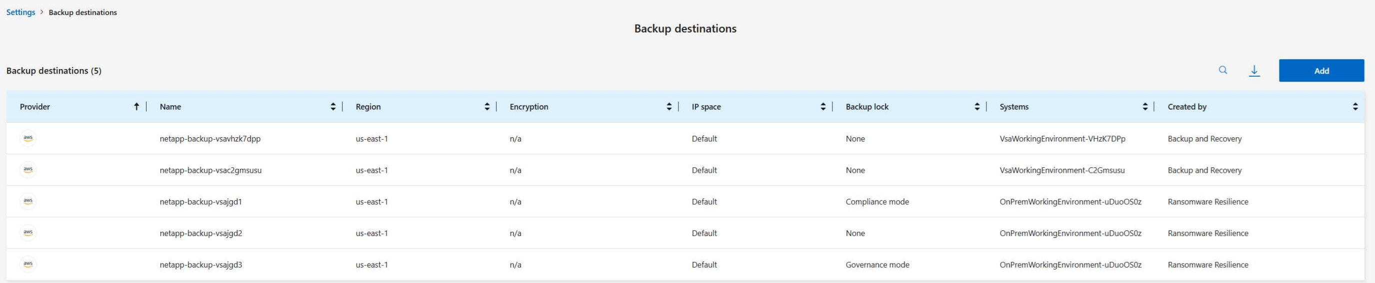
      Data in the account is encrypted with Microsoft-managed keys by default. You can continue to use Microsoft-managed keys, or you can manage the encryption of your data using your own keys.
    - **Networking**: Choose the IPspace and whether you’ll be using a Private Endpoint.
        - The IPspace is the cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
        - Optionally, choose whether you’ll use an Azure private endpoint that you previously configured.

          If you want to use Azure PrivateLink, refer to Azure PrivateLink.

5. Select **Add**.

Result

The new backup destination is added to the list of backup destinations.



Backup destinations (5)

Provider	Name	Region	Encryption	IP space	Backup lock	Systems	Created by
aws	netapp-backup-vsavhzk7dpp	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VHzK7DPp	Backup and Recovery
aws	netapp-backup-vsac2gmsusu	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsusu	Backup and Recovery
aws	netapp-backup-vsajgd1	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuoOS0z	Ransomware Resilience
aws	netapp-backup-vsajgd2	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuoOS0z	Ransomware Resilience
aws	netapp-backup-vsajgd3	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuoOS0z	Ransomware Resilience

Connect to a security and event management system (SIEM) for threat analysis and detection

You can automatically send data to your security and event management system (SIEM) for threat analysis and detection. You can select the AWS Security Hub, Microsoft Sentinel, or Splunk Cloud as your SIEM.

Before you enable SIEM in Ransomware Resilience, you need to configure your SIEM system.

About the event data sent to a SIEM

Ransomware Resilience can send the following event data to your SIEM system:

- **context**:
  - **os**: This is a constant with the value of ONTAP.
  - **os_version**: The version of ONTAP running on the system.
  - **connector_id**: The ID of the Console agent managing the system.
  - **cluster_id**: The cluster ID reported by ONTAP for the system.
  - **svm_name**: The name of the SVM where the alert was found.
  - **volume_name**: The name of the volume on which the alert is found.
  - **volume_id**: The ID of the volume reported by ONTAP for the system.
- **incident**:
  - **incident_id**: The incident ID generated by Ransomware Resilience for the volume under attack in Ransomware Resilience.
  - **alert_id**: The ID generated by Ransomware Resilience for the workload.
  - **severity**: One of the following alert levels: "CRITICAL", "HIGH", "MEDIUM", "LOW".
  - **description**: Details about the alert that was detected, for example, "A Potential ransomware attack detected on workload arp_learning_mode_test_2630"

Configure AWS Security Hub for threat detection

Before you enable AWS Security Hub in Ransomware Resilience, you'll need to do the following high level steps in AWS Security Hub:

- Set up permissions in AWS Security Hub.

- Set up the authentication access key and secret key in AWS Security Hub. (These steps are not provided here.)

Steps to set up permissions in AWS Security Hub

1. Go to **AWS IAM console**.
2. Select **Policies**.
3. Create a policy using the following code in JSON format:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

Configure Microsoft Sentinel for threat detection

Before you enable Microsoft Sentinel in Ransomware Resilience, you'll need to do the following high level steps in Microsoft Sentinel:

- **Prerequisites**
    - Enable Microsoft Sentinel.
    - Create a custom role in Microsoft Sentinel.
- **Registration**
    - Register Ransomware Resilience to receive events from Microsoft Sentinel.
    - Create a secret for the registration.
- **Permissions**: Assign permissions to the application.
- **Authentication**: Enter authentication credentials for the application.

Steps to enable Microsoft Sentinel

1. Go to Microsoft Sentinel.
2. Create a **Log Analytics workspace**.
3. Enable Microsoft Sentinel to use the Log Analytics workspace you just created.

Steps to create a custom role in Microsoft Sentinel

1. Go to Microsoft Sentinel.
2. Select **Subscription** > **Access control (IAM)**.
3. Enter a Custom role name. Use the name **Ransomware Resilience Sentinel Configurator**.
4. Copy the following JSON and paste it into the **JSON** tab.

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes":["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. Review and save your settings.

Steps to register Ransomware Resilience to receive events from Microsoft Sentinel

1. Go to Microsoft Sentinel.
2. Select **Entra ID** > **Applications** > **App registrations**.
3. For the **Display name** for the application, enter "**Ransomware Resilience**".
4. In the **Supported account type** field, select **Accounts in this organizational directory only**.
5. Select a **Default Index** where events will be pushed.
6. Select **Review**.
7. Select **Register** to save your settings.

   After registration, the Microsoft Entra admin center displays the application Overview pane.

Steps to create a secret for the registration

1. Go to Microsoft Sentinel.
2. Select **Certificates & secrets** > **Client secrets** > **New client secret**.
3. Add a description for your application secret.
4. Select an **Expiration** for the secret or specify a custom lifetime.

   A client secret lifetime is limited to two years (24 months) or less. Microsoft recommends that you set an expiration value of less than 12 months.

5. Select **Add** to create your secret.
6. Record the secret to use in the Authentication step. The secret is never displayed again after you leave this page.

Steps to assign permissions to the application

1. Go to Microsoft Sentinel.

2. Select **Subscription** > **Access control (IAM)**.
3. Select **Add** > **Add role assignment**.
4. For the **Privileged administrator roles** field, select **Ransomware Resilience Sentinel Configurator**.

   This is the custom role that you created earlier.

5. Select **Next**.
6. In the **Assign access to** field, select **User, group, or service principal**.
7. Select **Select Members**. Then, select **Ransomware Resilience Sentinel Configurator**.
8. Select **Next**.
9. In the **What user can do** field, select **Allow user to assign all roles except privileged administrator roles Owner, UAA, RBAC (Recommended)**.
10. Select **Next**.
11. Select **Review and assign** to assign the permissions.

Steps to enter authentication credentials for the application

1. Go to Microsoft Sentinel.
2. Enter the credentials:
   a. Enter the tenant ID, the client application ID, and the client application secret.
   b. Click **Authenticate**.

      After the authentication is successful, an "Authenticated" message appears.

3. Enter the Log Analytics workspace details for the application.
   a. Select the subscription ID, the resource group, and the Log Analytics workspace.

Configure Splunk Cloud for threat detection

Before you enable Splunk Cloud in Ransomware Resilience, you'll need to do the following high level steps in Splunk Cloud:

- Enable an HTTP Event Collector in Splunk Cloud to receive event data via HTTP or HTTPS from the Console.
- Create an Event Collector token in Splunk Cloud.

Steps to enable an HTTP Event Collector in Splunk

1. Go to Splunk Cloud.
2. Select **Settings** > **Data Inputs**.
3. Select **HTTP Event Collector** > **Global Settings**.
4. On the All Tokens toggle, select **Enabled**.
5. To have the Event Collector listen and communicate over HTTPS rather than HTTP, select **Enable SSL**.
6. Enter a port in **HTTP Port Number** for the HTTP Event Collector.

Steps to create an Event Collector token in Splunk

1. Go to Splunk Cloud.
2. Select **Settings** > **Add Data**.
3. Select **Monitor** > **HTTP Event Collector**.
4. Enter a Name for the token and select **Next**.
5. Select a **Default Index** where events will be pushed, then select **Review**.
6. Confirm that all settings for the endpoint are correct, then select **Submit**.
7. Copy the token and paste it in another document to have it ready for the Authentication step.

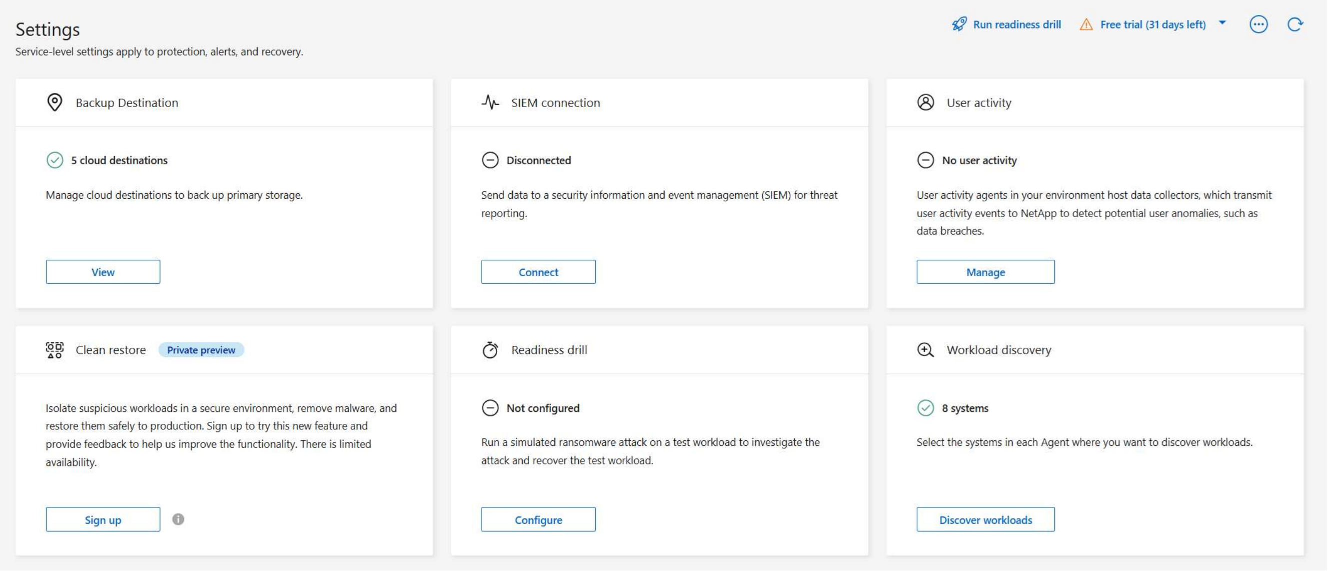
Connect SIEM in Ransomware Resilience

Enabling SIEM sends data from Ransomware Resilience to your SIEM server for threat analysis and reporting.

Steps

1. From the Console menu, select **Protection** > **Ransomware Resilience**.
2. From the Ransomware Resilience menu, select the vertical ⋮ … option at the top right.
3. Select **Settings**.

   The Settings page appears.



Settings

Service-level settings apply to protection, alerts, and recovery.

Backup Destination

5 cloud destinations

Manage cloud destinations to back up primary storage.

SIEM connection

Disconnected

Send data to a security information and event management (SIEM) for threat reporting.

User activity

No user activity

User activity agents in your environment host data collectors, which transmit user activity events to NetApp to detect potential user anomalies, such as data breaches.

Clean restore

Isolate suspicious workloads in a secure environment, remove malware, and restore them safely to production. Sign up to try this new feature and provide feedback to help us improve the functionality. There is limited availability.

Readiness drill

Not configured

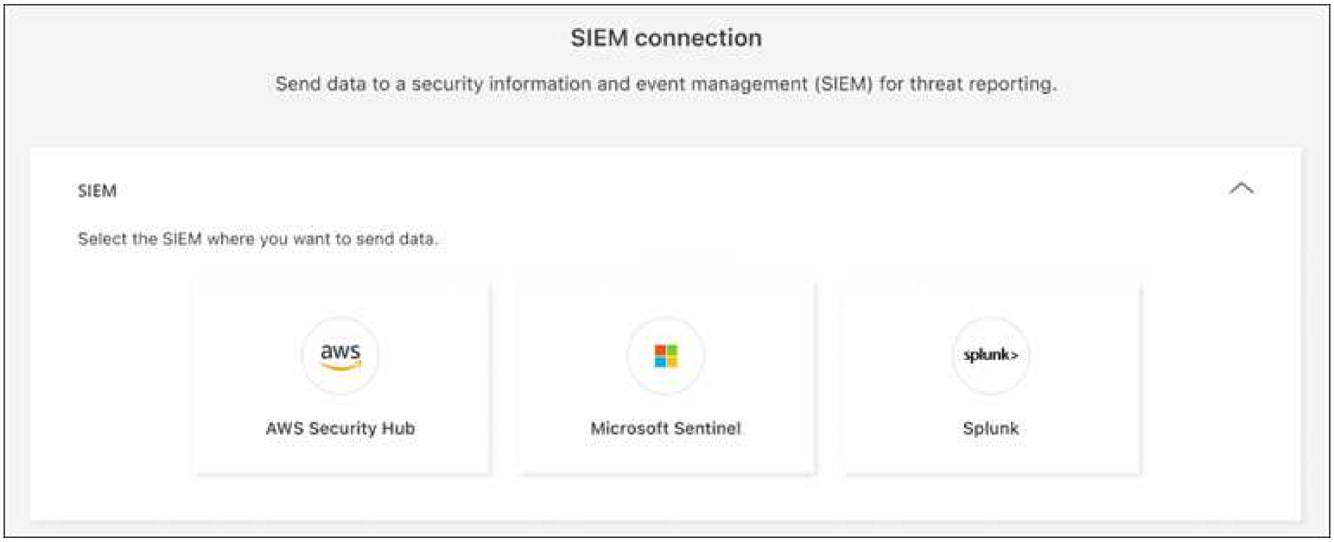
Run a simulated ransomware attack on a test workload to investigate the attack and recover the test workload.

Workload discovery

8 systems

Select the systems in each Agent where you want to discover workloads.

4. In the Settings page, select **Connect** in the SIEM connection tile.



SIEM connection

Send data to a security information and event management (SIEM) for threat reporting.

SIEM

Select the SIEM where you want to send data.

5. Choose one of the SIEM systems.
6. Enter the token and authentication details you configured in AWS Security Hub or Splunk Cloud.

   > The information that you enter depends on the SIEM you selected.

7. Select **Enable**.

   The Settings page shows "Connected."

Configure suspicious user activity detection in NetApp Ransomware Resilience

Ransomware Resilience supports detection of suspicious user behavior in detection policies, enabling you to address ransomware incidents at the user-level.

Ransomware Resilience detects suspicious user activity by analyzing user activity events generated by FPolicy in ONTAP. To collect user activity data, you need to deploy one or more user activity agents. The agent is a Linux server or VM with connectivity to devices on your tenant.

Agents and collectors

At least one user activity agent must be installed to activate suspicious user activity detection in Ransomware Resilience. When you activate the suspicious user activity feature from Ransomware Resilience dashboard, you need to provide the agent host information to activate the feature.

An agent can host multiple data collectors. Data collectors send data to a SaaS location for analysis. There are two types of collectors:

- The **data collector** collects user activity data from ONTAP.
- The **user directory connector** connects to your directory to map user IDs to usernames.

Collectors are configured in the Ransomware Resilience settings.

Enable suspicious user activity detection

Required Console role
To activate suspicious user activity detection, you need the Organization admin role. For subsequent configurations for suspicious user activity, you need the Ransomware Resilience user behavior admin role. Learn about Ransomware Resilience roles for NetApp Console.

Add a user activity agent

User activity agents are executable environments for data collectors; data collectors share user activity events with Ransomware Resilience. You must create at least one user activity agent to enable suspicious user activity detection.

Requirements

To install a user activity agent, you need a host or VM that meets the following supported operating system and server requirements.

Operating system requirements

Operating system	Supported versions
AlmaLinux	9.4 (64 bit) through 9.5 (64 bit), and 10 (64 bit), including SELinux
CentOS	CentOS Stream 9 (64 bit)
Debian	11 (64 bit), 12 (64 bit), including SELinux
OpenSUSE Leap	15.3 (64 bit) through 15.6(64 bit)
Oracle Linux	8.10 (64 bit), and 9.1 (64 bit) through 9.6 (64 bit), including SELinux
RedHat	8.10 (64 bit), 9.1 (64 bit) through 9.6 (64 bit), and 10 (64 bit), including SELinux
Rocky	Rocky 9.4 (64 bit) through 9.6(64 bit), including SELinux
SUSE Enterprise Linux	15 SP4 (64 bit) through 15 SP6 (64 bit), including SELinux
Ubuntu	20.04 LTS (64 bit), 22.04 LTS (64 bit) and 24.04 LTS (64 bit)

Server requirements

The server must meet the following minimum requirements:

- **CPU**: 4 CORES
- **RAM**: 16GB RAM
- **Disc space**: 35 GB free disk space

Cloud provider support

Suspicious user activity data can be stored in AWS and Azure in the following regions:

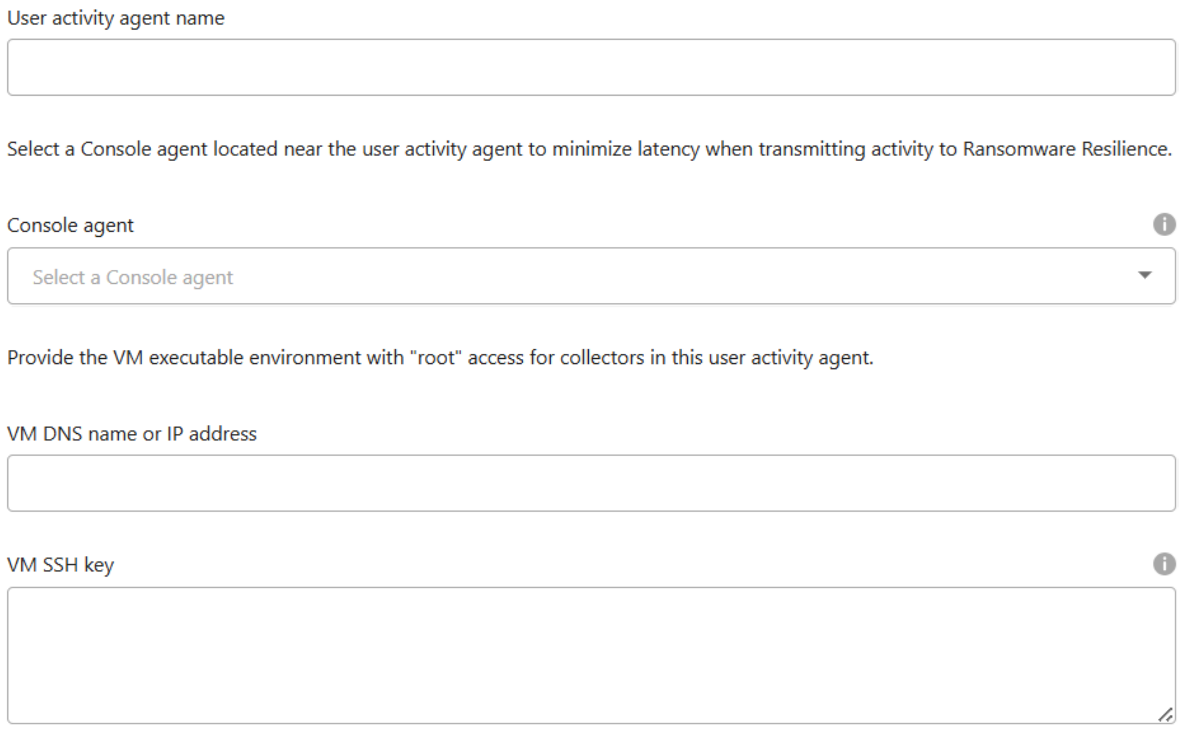
Cloud provider	Region
AWS	• Asia Pacific (Sydney) (ap-southeast-2) • Europe (Frankfurt) (eu-central-1) • US East (N. Virginia) (us-east-1)
Azure	East US

Steps

1. If this is your first time creating a user activity agent, go to the **Dashboard**. In the **User activity** tile, select **Activate**.

   If you're adding an additional user activity agent, go to **Settings**, locate the **User activity** tile, then select **Manage**. On the User activity screen, select the **User activity agents** tab then **Add**.

2. Select a **Cloud provider** then a **Region**. Select **Next**.
3. Provide the user activity agent details:
   - **User activity agent name**
   - **Console agent** - the Console agent should be in the same network as the user activity agent and have SSH connectivity to the user activity agent IP address.
   - **VM DNS name or IP address**
   - **VM SSH Key**



User activity agent name

Select a Console agent located near the user activity agent to minimize latency when transmitting activity to Ransomware Resilience.

Console agent

Select a Console agent

Provide the VM executable environment with "root" access for collectors in this user activity agent.

VM DNS name or IP address

VM SSH key

4. Select **Next**.
5. Review your settings. Select **Activate** to complete adding the user activity agent.

6. Confirm the user activity agent was successfully created. In the User activity tile, a successful deployment displays as Running.

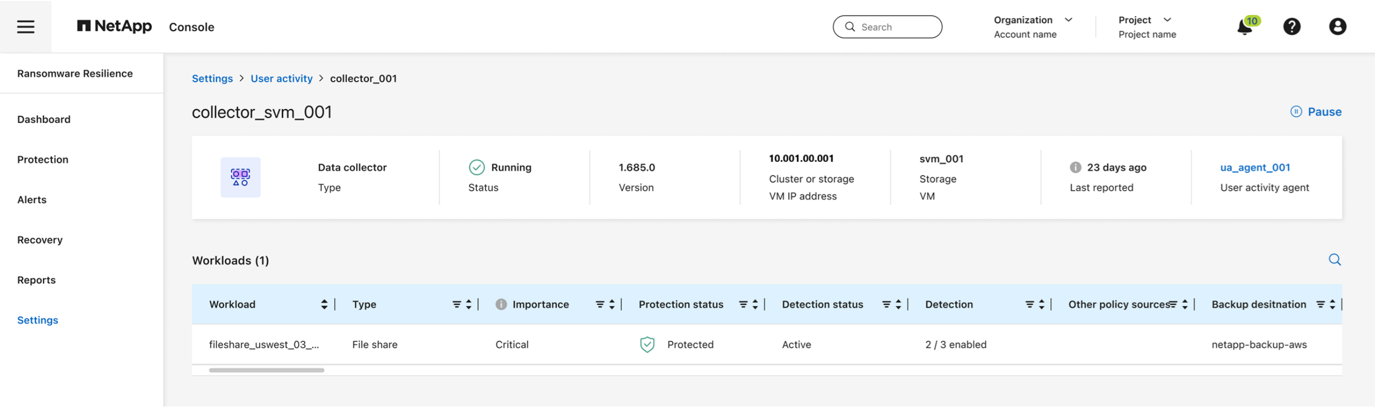
Result

After the user activity agent is successfully created, return to the **Settings** menu then select **Manage** in the User activity tile. Select the **User activity agent** tab then select the user activity agent to view details about it, including data collectors and user directory connectors.

Add a data collector

Data collectors are created automatically when you enable a ransomware protection strategy with suspicious user activity detection. For more information, see add a detection policy.

You can view the details of the data collector. From Settings, select **Manage** in the User activity tile. Select the **Data collector** tab then select the data collector to view its details or pause it.



Settings > User activity > collector_001

collector_svm_001

Data collector Type	Running Status	1.685.0 Version	10.001.00.001 Cluster or storage VM IP address	svm_001 Storage VM	23 days ago Last reported	ua_agent_001 User activity agent

Workloads (1)

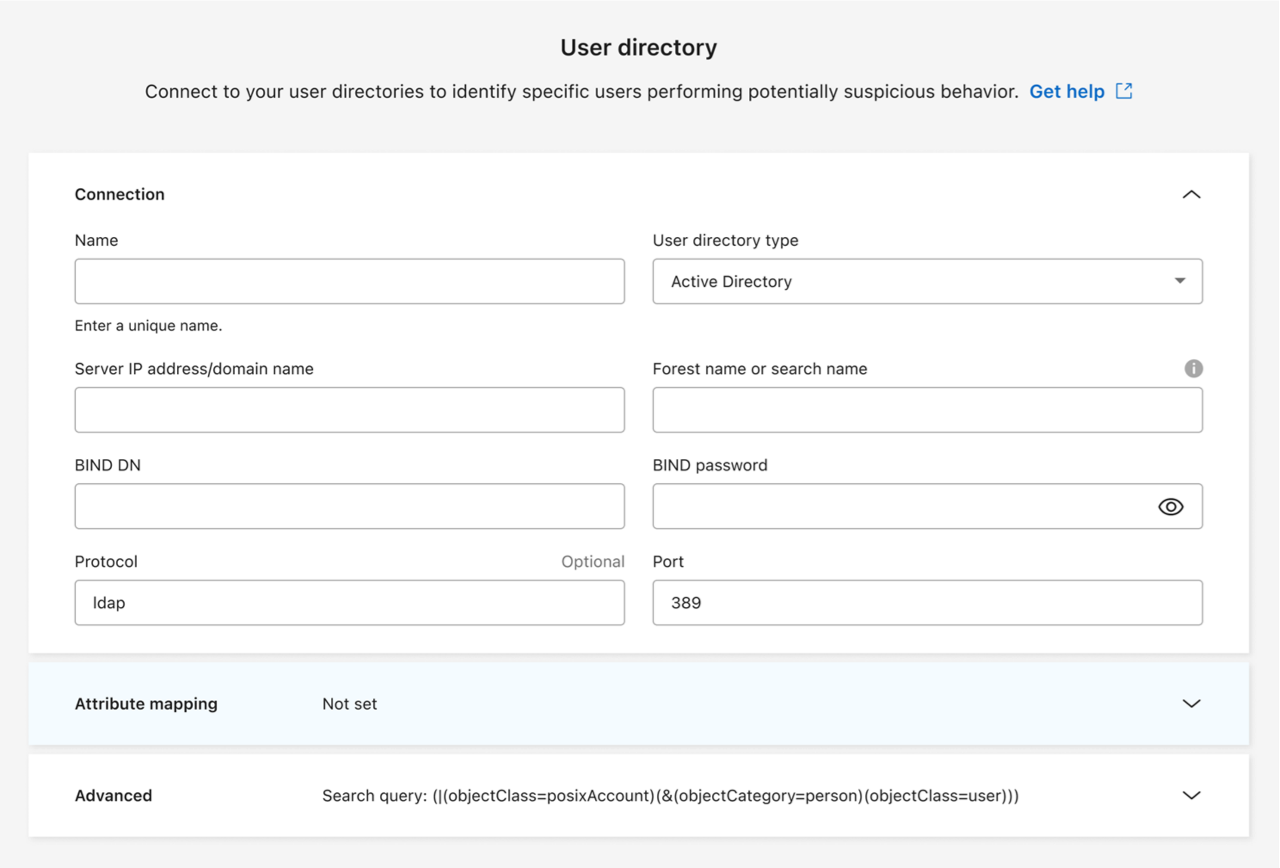
Workload	Type	Importance	Protection status	Detection status	Detection	Other policy sources	Backup desitnation
fileshare_uswest_03_...	File share	Critical	Protected	Active	2 / 3 enabled		netapp-backup-aws

Add a user directory connector

To map user IDs to usernames, you must create a user directory connector.

Steps

1. In Ransomware Resilience, go to **Settings**.
2. In the User activity tile, select **Manage**.
3. Select the **User directory connectors** tab then **Add**.
4. Provide the details of the connection:
   - **Name**
   - **User directory type**
   - **Server IP address or domain name**
   - **Forest name or search name**
   - **BIND domain name**
   - **BIND password**
   - **Protocol** (this is optional)
   - **Port**



User directory

Connect to your user directories to identify specific users performing potentially suspicious behavior. Get help

Connection

Name

Enter a unique name.

User directory type: Active Directory

Server IP address/domain name

Forest name or search name

BIND DN

BIND password

Protocol (Optional): ldap

Port: 389

Attribute mapping: Not set

Advanced: Search query: (|(objectClass=posixAccount)(&(objectCategory=person)(objectClass=user)))

Provide the attribute mapping details:

- **Display name**
- **SID** (if you’re using LDAP)
- **User name**
- **Unix ID** (if you’re using NFS)
- Select **Include optional attributes**. You can also include email address, telephone number, role, state, country, department, photo, manager DN, or groups.

Select **Advanced** to add an optional search query.

5. Select **Add**.
6. Return to the user directory connectors tab to check the status of your user directory connector. If created successfully, the status of the user directory connector displays as **Running**.

Delete a user directory connector

1. In Ransomware Resilience, go to **Settings**.
2. Locate the User activity tile, select **Manage**.
3. Select the **User directory connector** tab.
4. Identify the user directory connector you want to delete. In the action menu at the end of the line, select the three dots … then **Delete**.
5. In the pop-up dialog, select **Delete** to confirm your actions.

Respond to suspicious user activity alerts

After you configure suspicious user activity detection, you can monitor events in the alerts page. For more information, see Detect malicious activity and anomalous user behavior.

Copyright information

Trademark information

[1] Although it’s possible that an attack might go undetected, our research indicates NetApp technology has resulted in a high degree of detection for certain file encryption-based ransomware attacks.